अखिल भारतीय तकनीकी शिक्षा परिषद द्वारा संचालित ''हिंदी में तकनीकी एवं प्रबंधन विषयों पर लिखी गई पाण्डुलिपियों के प्रकाशन हेतु वित्तीय सहायता योजना'' के अंतर्गत प्रस्तुत संशोधित पाण्डुलिपि

क्रिप्टोग्राफी और नेटवर्क सुरक्षा

द्वारा

डॉ. एस. एस. श्रीवास्तव
(एम. एस–सी., पीएच. डी., पी. जी. डी. सी. ए.)
गणित विभाग
उच्च शिक्षा उत्कृष्टता संस्थान, भोपाल (म. प्र.)
मोबाइलः 9425362906
ई–मेल : sss.math@yahoo.co.in

भूमिका

इलेक्ट्रॉनिक ईवसड्रॉपिंग और इलेक्ट्रॉनिक धोखाधड़ी के वायरस और हैकर्स के इस युग में, सुरक्षा सर्वोपरि है। जैसा कि क्रिप्टोग्राफी और नेटवर्क सुरक्षा के विषयों में परिपक्व हो गए हैं, नेटवर्क सुरक्षा को लागू करने के लिए अधिक व्यावहारिक, आसानी से उपलब्ध अनुप्रयोग विकसित हुए हैं। यह पुस्तक क्रिप्टोग्राफी और नेटवर्क सुरक्षा के सिद्धांतों और अभ्यास दोनों का व्यावहारिक सर्वेक्षण प्रदान करता है।

सार्वभौमिक इलेक्ट्रॉनिक कनेक्टिविटी के इस युग में, वायरस और हैकर्स की, इलेक्ट्रॉनिक ईवसड्रॉपिंग और इलेक्ट्रॉनिक धोखाधड़ी की, वास्तव में कोई समय नहीं है जिस पर सुरक्षा कोई फर्क नहीं पड़ता। इस पुस्तक के महत्वपूर्ण हित के विषय को बनाने के लिए दो रुझान आए हैं। सबसे पहले, कंप्यूटर सिस्टम में विस्फोटक वृद्धि और नेटवर्क के माध्यम से उनके अंतर्संबंधों ने इन प्रणालियों का उपयोग करके संग्रहीत और संचारित सूचनाओं पर दोनों संगठनों और व्यक्तियों की निर्भरता में वृद्धि की है। बदले में, डेटा और संसाधनों को प्रकटीकरण से बचाने की आवश्यकता के बारे में जागरूकता बढ़ाने के लिए, गारंटी देने के लिए प्रेरित किया है

डेटा और संदेशों की प्रामाणिकता, और सिस्टम को नेटवर्क–आधारित हमलों से बचाने के लिए। दूसरा, क्रिप्टोग्राफी और नेटवर्क सुरक्षा के विषय परिपक्व हो गए हैं, जिससे नेटवर्क सुरक्षा को लागू करने के लिए व्यावहारिक, आसानी से उपलब्ध अनुप्रयोगों का विकास हो रहा है।

क्रिप्टोग्राफी और नेटवर्क सुरक्षा के सिद्धांतों और व्यवहार दोनों का व्यावहारिक सर्वेक्षण प्रदान करना इस पुस्तक का उद्देश्य है। पुस्तक के प्रथम भाग में, नेटवर्क सुरक्षा क्षमता द्वारा संबोधित किए जाने वाले बुनियादी मुद्दों को क्रिप्टोग्राफी और नेटवर्क सुरक्षा तकनीक का एक ट्यूटोरियल और सर्वेक्षण प्रदान करके पता लगाया जाता है। पुस्तक का उत्तरार्द्ध नेटवर्क सुरक्षा के अभ्यास से संबंधित है, व्यावहारिक अनुप्रयोग जो लागू किए गए हैं और नेटवर्क सुरक्षा प्रदान करने के लिए उपयोग में हैं। पुस्तक को स्व–निहित बनाने का प्रयास किया गया है। पुस्तक न केवल आवश्यक गणितीय परिणामों को प्रस्तुत करती है, बल्कि पाठक को उन परिणामों की सहज समझ प्रदान करती है।

पुस्तक एक अकादमिक और एक पेशेवर पाठक दोनों के लिए है। एक पाठ्यपुस्तक के रूप में, यह कंप्यूटर विज्ञान, कंप्यूटर इंजीनियरिंग और इलेक्ट्रिकल इंजीनियरिंग के स्नातक/परा–स्नातक विद्यार्थियों के लिए उनके पाठ्यक्रम के अनुरूप उपयोगी हो सकती है।

प्रस्तावित पुस्तक में क्रिप्टोग्राफी के विज्ञान की मूल बातें शामिल की गई हैं। यह बताता है कि कम्प्यूटर डेटा की गोपनीयता बनाए रखने के लिए प्रोग्रामर और नेटवर्क पेशेवर क्रिप्टोग्राफी का उपयोग कैसे कर सकते हैं। क्रिप्टोग्राफी की उत्पत्ति से शुरू, यह क्रिप्टोसिस्टम, विभिन्न पारंपरिक और आधुनिक सिफर, सार्वजनिक कुंजी एन्क्रिप्शन, डेटा एकीकरण, संदेश प्रमाणीकरण, और डिजिटल हस्ताक्षर समझाता है। यह पुस्तक कम्प्यूटर विज्ञान के उन छात्रों के लिए है जो क्रिप्टोग्राफी की मूल बातें सीखने की इच्छा रखते हैं। यह नेटवर्किंग पेशेवरों के लिए भी उपयोगी होगा जो अपने नेटवर्क पर सुरक्षित डेटा संचार सुनिश्चित करने के लिए विभिन्न क्रिप्टोग्राफिक एल्गोरिथ्म को शामिल करना चाहते हैं।

नेटवर्क सुरक्षा नेटवर्क पर मौजूद संवेदनशील सूचना संपत्तियों की सुरक्षा से संबंधित सभी पहलुओं से संबंधित है। इसमें डेटा संचार के लिए मौलिक सुरक्षा सेवाएं प्रदान करने के लिए विकसित विभिन्न तंत्र शामिल हैं। यह पुस्तक कई प्रकार के नेटवर्क भेद्यता और हमलों के खिलाफ नियोजित सुरक्षा उपायों के विवरण को बताता है। यह एप्लिकेशन से डेटा लिंक परत तक विभिन्न नेटवर्किंग परतों पर नियोजित सबसे आम सुरक्षा प्रोटोकॉल के कामकाज का वर्णन करता है। इस पुस्तक के माध्यम से छात्र नेटवर्क सुरक्षा के बारे में ज्ञान के मध्यवर्ती स्तर पर पाएंगे। यह पुस्तक शुरुआती लोगों के लिए नेटवर्क सुरक्षा की मूल बातें समझने में सहायक होगा। जो सूचना और नेटवर्क सुरक्षा के क्षेत्र में कैरियर लेने के इच्छुक हैं, यह पुस्तक उनके लिए उपयोगी होगी।

प्रस्तुत प्रस्ताव में पुस्तक को 2 भागों और 13 अध्याओं में बांटा गया है। प्रथम भाग क्रिप्टोग्राफी और द्वितीय भाग नेटवर्क सुरक्षा की अभिकल्पना को विस्तारित करता है। पुस्तक के अंत में एक परिशिष्ट जिसमें विजुअल क्रिप्टोग्राफी और क्वांटम क्रिप्टोग्राफी की अवधारणा को सम्मिलित किया गया है जो कि भविष्य में सुरक्षा की दृष्टिकोण से आवश्यक चरण हैं। सबसे अंत में आवश्यक शब्दावली और संदर्भ ग्रंथों की सूची शामिल है। प्रत्येक अध्याय के अंत में प्रश्नों का एक संकलन दिया गया है। विद्यार्थियों की सुविधा की

दृष्टिकोण से पुस्तक में प्रचलित तकनीकी शब्दों को उनके मूल रूप के साथ–साथ 'कंप्यूटर विज्ञान शब्दावली' में दिए गए उनके हिन्दी अर्थों को भी सम्मिलित किया गया है।

इस पुस्तक में भारत सरकार द्वारा प्रकाशित 'वृहत् पारिभाषिक शब्द–संग्रह विज्ञानः खण्ड 1 और 2' तथा 'कंप्यूटर विज्ञान शब्दावली' से वैज्ञानिक शब्दावली को लिया गया है। आशा है कि यह पुस्तक छात्र/छात्राओं की समस्त वांछित आवश्यकताओं की पूर्ति करने में सक्षम होगी। प्रस्तुत पुस्तक में दिए गए चित्रों में से कुछ चित्र इंटरनेट से लिए गए हैं जिसके लिए लेखक आभारी है।

प्रथम अध्याय में **क्रिप्टोग्राफी – एक परिचय** दिया गया है। द्वितीय अध्याय में **क्लासिकल एन्क्रिप्शन** को समझाया गया है। **एन्क्रिप्शन स्टैंडर्ड** को तृतीय अध्याय में रखा गया है। **ऑपरेशन के ब्लॉक सिफर मोड्स** का समावेश चतुर्थ अध्याय में किया गया है। पंचम अध्याय **पब्लिक की एन्क्रिप्शन** की अभिकल्पना को विस्तारित करता है। **हैश फंक्शन** को षष्ठम् अध्याय में रखा गया है। सप्तम अध्याय में **डिजिटल सिग्नेचर** को समझाया गया है। अष्टम अध्याय में **नेटवर्क सुरक्षा – एक आकलन** की अभिकल्पना को विस्तारित किया गया है। नवम् अध्याय में **एप्लीकेशन लेयर** को समझाया गया है। **ट्रांसपोर्ट लेयर** को दशम् अध्याय में रखा गया है। एकादश अध्याय **नेटवर्क लेयर** की अभिकल्पना को विस्तारित करता है। **डाटा लिंक लेयर** का समावेश द्वादश अध्याय में किया गया है। त्रायोदश अध्याय में **एक्सेस कन्ट्रोल और फायरवॉल** को समझाया गया है।

लेखक

क्रिप्टोग्राफी और नेटवर्क सुरक्षा

विषय सूची

भाग – 1 : क्रिप्टोग्राफी

अध्याय – 1 : क्रिप्टोग्राफी (कूटलेखन) – एक परिचय 1–23

1.1 क्रिप्टोग्राफी (कूटलेखन) की उत्पत्ति
1.2 क्रिप्टैनालिसिस (कूटविश्लेषण)
1.3 क्रिप्टोलॉजी (कूटलिपि)
1.4 स्टेग्नोग्राफी (गुप्त लेखन)
1.5 क्रिप्टोग्राफी (कूटलेखन) का इतिहास
    1.5.1 क्रिप्टोग्राफी (कूटलेखन) का विकास
    1.5.2 प्राचीनकाल क्रिप्टोग्राफी (कूटलेखन)
    1.5.3 मध्यकालीन क्रिप्टोग्राफी (कूटलेखन)
    1.5.4 1800 से द्वितीय विश्व युद्व तक क्रिप्टोग्राफी (कूटलेखन)
    1.5.5 आधुनिक क्रिप्टोग्राफी (कूटलेखन)
1.6 क्रिप्टोग्राफी (कूटलेखन) का संदर्भ
1.7 क्रिप्टोग्राफी (कूटलेखन) की सुरक्षा सेवायें
1.8 क्रिप्टोग्राफी (कूटलेखन) प्राथिमिकी
1.9 क्रिप्टोसिस्टम (कूटप्रणाली)
1.10 क्रिप्टोसिस्टम (कूटप्रणाली) की शक्ति
1.11 क्रिप्टोसिस्टम (कूटप्रणाली) का लक्ष्य
    1.11.1 क्रिप्टोसिस्टम (कूटप्रणाली) के घटक
    1.11.2 क्रिप्टोसिस्टम (कूटप्रणाली) के प्रकार
    1.11.3 सममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया)
    1.11.4 असममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया)
1.12 सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) की चुनौती
1.13 क्रिप्टोसिस्टम (कूटप्रणाली) के लिए केर्कहोफ का सिद्धांत
1.14 क्रिप्टोसिस्टम (कूटप्रणाली) पर आक्रमण
1.15 क्रिप्टोग्राफिक (कूटलेखीय) आक्रमण
1.16 क्रिप्टोग्राफी (कूटलेखन) गुण और दोष
1.17 क्रिप्टोग्राफी (कूटलेखन) के अनुप्रयोग
1.18 क्रिप्टोग्राफी (कूटलेखन) का भविष्य

अध्याय – 2 : प्राचीनकाल एन्क्रिप्शन (कूट प्रक्रिया) 24–56

2.1 सीजर या विस्थापन सिफर (कूटलेख)
2.2 सरल प्रतिस्थापन सिफर (कूटलेख)
2.3 मोनोअल्फाबेटिक और पॉलीअल्फाबेटिक सिफर (कूटलेख)
2.4 प्लेफेयर सिफर (कूटलेख)
2.5 विगेनियर सिफर (कूटलेख)

2.6 ट्रान्सपोजीशन सिफर (कूटलेख)
2.7 एफिन सिफर (कूटलेख)
2.8 निहिलिस्ट सिफर (कूटलेख)
2.9 प्रोडक्ट सिफर (कूटलेख)
2.10 हिल सिफर (कूटलेख)
2.11 विभिन्न विधियों के लिए कम्प्यूटर प्रोग्राम

अध्याय – 3 : एन्क्रिप्शन स्टैंडर्ड (कूटित मानक) 57–77

3.1 आधुनिक सममित कुंजी एन्क्रिप्शन (कूटित)
  3.1.1 ब्लॉक सिफर (खण्ड कूटलेख)
  3.1.2 स्ट्रीम सिफर (प्रवाह कूटलेख)
3.2 डाटा एन्क्रिप्शन स्टैंडर्ड (आँकड़ा कूटित मानक)
3.3 एडवांस्ड एन्क्रिप्शन स्टैंडर्ड (उन्नत कूटित मानक)
3.4 इन्टरनेशनल डाटा एन्क्रिप्शन एल्गोरिथम
3.5 त्रिक DES

अध्याय – 4 : ऑपरेशन के ब्लॉक सिफर (खण्ड कूटलेख) मोड्स 78–92

4.1 इलेक्ट्रॉनिक कोड बुक मोड (ECB)
4.2 सिफर ब्लॉक (कूटलेख खण्ड) चेनिंग मोड (CBC)
4.3 सिफर (कूटलेख) फीडबैक मोड (CFB)
4.4 आउटपुट फीडबैक मोड (OFB)
4.5 काउन्टर (गणित्र) मोड (CTR)
4.6 ब्लॉक सिफर (खण्ड कूटलेख) के लाभ और नुकसान

अध्याय – 5 : पब्लिक की एन्क्रिप्शन (सार्वजनिक कुंजी कूट प्रक्रिया) 93–115

5.1 पब्लिक की क्रिप्टोग्राफी (सार्वजनिक कुंजी कूटेखन)
5.2 RSA क्रिप्टोसिस्टम (कूटप्रणाली)
5.3 ElGamal क्रिप्टोसिस्टम (कूटप्रणाली)
5.4 एलिप्टिक–कर्व क्रिप्टोग्राफी (अण्डाकार–वक्र कूटलेखन) (ECC)
5.5 संयोजन तकनीकः सिमेट्रिक और असिमेट्रिक एन्क्रिप्शन (सममित और असममित कूट प्रक्रिया)

अध्याय – 6 : हैश फंक्शन (द्रुतान्वेषण फलन) 116–132

6.1 क्रिप्टोग्राफी हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन)
6.2 हैश फंक्शन (द्रुतान्वेषण फलन) की विशेषतायें
6.3 हैश फंक्शन (द्रुतान्वेषण फलन) के प्रगुण
6.4 हैशिंग एल्गोरिथम (द्रुतान्वेषण कलन विधि) की अभिकल्पना
6.5 प्रसिद्व हैश फंक्शन (द्रुतान्वेषण फलन)
  6.5.1 मैसेज डाइजेस्ट (संदेश संग्रह) (MD)
  6.5.2 सुरक्षित हैश फंक्शन (द्रुतान्वेषण फलन) (SHA)
  6.5.3 RIPEMD
  6.5.4 व्हर्लपूल
6.6 हैश फंक्शन (द्रुतान्वेषण फलन) के अनुप्रयोग
6.7 संदेश प्रमाणीकरण
6.8 चेकसम (जाँच योग)

अध्याय – 7 : डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) 133–147

7.1 क्रिप्टोग्राफी डिजिटल सिग्नेचर (कूटलेखन अंकीय हस्ताक्षर)
7.2 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) का प्रारूप
7.3 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) का महत्व
7.4 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) के साथ एन्क्रिप्शन (कूट प्रक्रिया)
7.5 पब्लिक की इन्फ्रास्ट्रक्चर (सार्वजनिक कुंजी अवसंरचना)
7.6 डिजिटल सर्टिफिकेट (अंकीय प्रमाण पत्र)
7.7 प्रमाणन प्राधिकरण (CA)
7.8 प्रमाणन प्राधिकरण का अनुक्रम
7.9 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) के अनुप्रयोग

भाग – 2 : नेटवर्क सुरक्षा

अध्याय – 8 : नेटवर्क सुरक्षा – एक आकलन 148–164

8.1 भौतिक नेटवर्क
8.2 नेटवर्क प्रोटोकॉल (संदेशाचार)
- 8.2.1 TCP/IP प्रोटोकॉल (संदेशाचार)
- 8.2.2 DNS प्रोटोकॉल (संदेशाचार)
- 8.2.3 ICMP प्रोटोकॉल (संदेशाचार)

8.3 नेटवर्क सुरक्षा के लक्ष्य
8.4 नेटवर्क सुरक्षा प्राप्त करना
8.5 नेटवर्क सुरक्षा की आवश्यकता

अध्याय – 9 : एप्लीकेशन लेयर (अनुप्रयोग परत) 165–178

9.1 ई–मेल सुरक्षा
9.2 ई–मेल सुरक्षा सेवायें
- 9.2.1 एक–से–एक ई–मेल
- 9.2.2 एक–से–बहुल प्राप्तकर्ता ई–मेल
- 9.2.3 एक–से–वितरण सूची ई–मेल

9.3 PGP
9.4 S/MIME
9.5 DNS सुरक्षा

अध्याय – 10 : ट्रांस्पोर्ट लेयर (परिवहन परत) 179–198

10.1 ट्रांस्पोर्ट लेयर (परिवहन परत) सुरक्षा की आवश्यकता
10.2 सिक्योर सॉकेट लेयर (सुरक्षित सॉकेट परत) (SSL)
10.3 TLS प्रोटोकॉल (संदेशाचार)
10.4 सिक्योर (सुरक्षित) ब्राउजिंग – HTTPS
10.5 सिक्योर शेल प्रोटोकॉल (सुरक्षित शेल संदेशाचार) (SSH)
10.6 लाभ और सीमायें

अध्याय – 11 : नेटवर्क लेयर (जालक्रम परत) 199–218

11.1 नेटवर्क लेयर (जालक्रम परत) में सुरक्षा
11.2 IPsec का आकलन
11.3 IPsec कम्यूनिकेशन (संचार) मोड
11.4 IPsec प्रोटोकॉल (संदेशाचार)
11.5 IPsec में सुरक्षा संघ

अध्याय – 12 : डेटा लिंक लेयर (आंकड़ा कड़ी परत) 219–233

12.1 डाटा लिंक लेयर (आंकड़ा कड़ी परत) में सुरक्षा
12.2 सुरक्षित ईथरनेट लैन
12.3 सुरक्षित स्पानिंग ट्री प्रोटोकॉल (सुरक्षित विस्तरित तरू संदेशाचार)
12.4 सुरक्षित आभासी लैन
12.5 सुरक्षित वायरलेस (बेतार) लैन

अध्याय – 13 : एक्सेस कन्ट्रोल (अभिगम नियंत्रण) और फायरवॉल 234–246

13.1 नेटवर्क उपकरणों तक पहुँच सुरक्षित करना
13.2 उपयोगकर्ता प्रमाणीकरण और प्रमाणन
13.3 पासवर्ड (पारण शब्द) आधारित प्रमाणीकरण
13.4 केन्द्रीकृत प्रमाणीकरण विधि
13.5 एक्सेस (अभिगम) नियंत्रण सूची
13.6 कम्प्यूटर वायरस
13.7 एण्टी वायरस
13.8 फायरवॉल
13.8.1 स्टेटलेस और स्टेटफुल पैकेट फिल्टरिंग फायरवॉल
13.8.2 अनुप्रयोग गेटवे (द्वार)
13.8.3 सर्किट लेवल गेटवे (परिपथ स्तरीय द्वार)
13.9 DMZ के साथ फायरवॉल परिनियोजन
13.10 रोकथाम प्रणाली
13.11 IDS के प्रकार

परिशिष्ट 247–251

1. विजुअल क्रिप्टोग्राफी
2. क्वांटम क्रिप्टोग्राफी

शब्द संग्रह
संदर्भ ग्रंथ

अध्याय – 1

क्रिप्टोग्राफी (कूटलेखन) – एक परिचय

1.1 क्रिप्टोग्राफी (कूटलेखन) की उत्पत्तिः

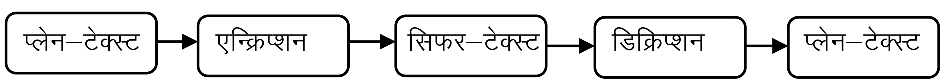
क्रिप्टोग्राफी (कूटलेखन) शब्द ग्रीक शब्द κρυπτο (छुपा या गुप्त) और γραφη (लेखन) से आता है। क्रिप्टोग्राफी (कूटलेखन) गुप्त लेखन की कला है। क्रिप्टोग्राफी (कूटलेखन) द्वारा प्रदान की जाने वाली मूल सेवा प्रतिभागियों के बीच जानकारी भेजने की क्षमता है जो दूसरों को इसे पढ़ने से रोकती है।

शब्द 'क्रिप्टोग्राफी' को दो ग्रीक शब्दों के संयोजन से बनाया गया था, 'क्रिप्टा' जिसका अर्थ है छिपा हुआ और 'ग्रैफेन' जिसका अर्थ है लेखन।

सदैव से मनुष्यों की दो अंतर्निहित जरूरतें थीं – (1) सूचना का संचार और साझा करना (2) चुने हुए व्यक्तियों के मध्य संचार करना। इन दोनों आवश्यकताओं ने संदेशों को कोडिंग (कूटन) करने की कला को जन्म दिया जिससे केवल वांछित व्यक्तियों के मध्य सूचना की पहुंच हो सके। अनाधिकृत लोग किसी भी सूचना को निकालने में असमर्थ थे, भले ही कूटित संदेश उन तक क्यों न पहुँच जाय।

सूचना की सुरक्षा में गुप्तता पेश करने के लिए संदेशों को छुपाने की कला और विज्ञान को क्रिप्टोग्राफी (कूटलेखन) के रूप में पहचाना जाता है। एक संदेश अपने मूल रूप में प्लेन–टेक्स्ट (plaintext) या क्लीयर–टेक्स्ट (cleartext) या साधारण–पाठ के रूप में जाना जाता है। कूटित सूचना को सिफर–टेक्स्ट (ciphertext) या कूटलेख–पाठ के रूप में जाना जाता है। प्लेन–टेक्स्ट (साधारण–पाठ) से सिफर–टेक्स्ट (कूटलेख–पाठ) बनाने की प्रक्रिया को एन्क्रिप्शन (encryption) या कूटित के रूप में जाना जाता है। एन्क्रिप्शन (कूटित) के विपरीत को डिक्रिप्शन (decryption) या अकूटित कहा जाता है।

एन्क्रिप्शन (कूटित), मूल डाटा जिसे प्लेन–टेक्स्ट या क्लीयर–टेक्स्ट या साधारण–पाठ कहा जाता है को उस रूप में परिवर्तित करने की एक विधि है, जो यादृच्छिक प्रकट होता है और अपठनीय प्रतीत होता है, और जिसे सिफर–टेक्स्ट (कूटलेख–पाठ) कहा जाता है। प्लेन–टेक्स्ट (साधारण–पाठ) या तो उस रूप में है जिसे किसी व्यक्ति या कम्प्यूटर (निष्पादन योग्य कोड) द्वारा समझा जा सकता है। एक बार यह सिफर–टेक्स्ट (कूटलेख–पाठ) में परिवर्तित हो जाने के बाद, न तो मनुष्य और न ही मशीन इसे ठीक से संसाधित कर सकती है जब तक कि इसे डिक्रिप्ट (अकूटित) नहीं किया जाता है।



(चित्र क्र0 1.1)

इस प्रकार क्रिप्टोग्राफी डेटा (कूटलेखन आँकड़ा) को उस रूप में संग्रहित और प्रसारित करने का एक तरीका है जिसे केवल वही व्यक्ति पढ़ और संसाधित कर सकते हैं जो इसे संयोजित करते हैं। यह एक अपठनीय प्रारूप में एन्कोडिंग (encoding) करके सूचना की सुरक्षा का विज्ञान है। क्रिप्टोग्राफी (कूटलेखन) संवेदनशील जानकारी की सुरक्षा का एक प्रभावी तरीका है क्योंकि यह माध्यम पर संग्रहीत है या नेटवर्क (जालक्रम) संचार पथ के माध्यम से प्रेषित होता है। क्रिप्टोग्राफी (कूटलेखन) के अनुप्रयोगों में एटीएम कार्ड, कम्प्यूटर पासवर्ड और इलेक्ट्रॉनिक वाणिज्य शामिल हैं।

क्रिप्टोग्राफी (कूटलेखन) ने अब वर्तमान में बड़े पैमाने पर उत्पाद बाजारों में प्रवेश किया है और विकसित देशों के हर नागरिक इसका दैनिक उपयोग करते हैं। इसका उपयोग प्रमाणीकरण और एन्क्रिप्शन (बैंक कार्ड, वायरलेस टेलीफोन, ई–कॉमर्स, पे–टीवी), एक्सेस कंट्रोल (कार लॉक सिस्टम, स्की लिफ्ट), भुगतान (प्रीपेड टेलीफोन कार्ड, ई–कैश) के लिए किया जाता है। यह ई–वोटिंग सिस्टम के साथ लोकतंत्र के साधन के रूप में और अधिक उपयोगी हो सकता है।

1.2 क्रिप्टैनालिसिस (कूटविश्लेषण):

क्रिप्टैनालिसिस (कूटविश्लेषण), आवश्यक गुप्त जानकारी तक पहुंच के बिना एन्क्रिप्टेड (कूटित) सूचना के अर्थ को प्राप्त करने के तरीकों का अध्ययन है। आम तौर पर, इसमें यह जाना जाता है कि सिस्टम कैसे कार्य करता है और एक गुप्त कुंजी (Key) भी ढूंढना शामिल है।

क्रिप्टैनालिसिस (कूटविश्लेषण) को कोड–ब्रेकिंग (Code-Braking) या कोड क्रैकिंग (Code-Cracking) के रूप में भी जाना जाता है। प्राप्त करने के लिए सिफर–टेक्स्ट (कूटलेख–पाठ) आमतौर पर क्रिप्टोसिस्टम (कूटतंत्र) का सबसे आसान भाग होता है और इसलिए यह क्रिप्टैनालिसिस (कूटविश्लेषण) का एक महत्वपूर्ण हिस्सा है। कोड (कूट), सिफर (कूटलेख) या एन्क्रिप्टेड टेक्स्ट (कूटित पाठ) का डिक्रिप्शन (अकूटन) और विश्लेषण क्रिप्टैनालिसिस (कूटविश्लेषण) कहलाता है। क्रिप्टैनालिसिस (कूटविश्लेषण), एल्गोरिथम (कलनविधि) भेद्यता की खोज करने और क्रिप्टोग्राफी (कूटलेखन) या सूचना सुरक्षा प्रणालियों में तोड़ने के लिए गणितीय सूत्रों का उपयोग करता है।

क्रिप्टैनालिसिस (कूटविश्लेषण) (ग्रीक से क्रिप्टोस (*kryptós*), छुपा (hidden), और एनालिनीन (*analýein*)) प्रणाली के छिपे पहलुओं का अध्ययन करने के लिए सूचना प्रणाली का विश्लेषण करने की कला और विज्ञान है। क्रिप्टोग्राफिक्स (कूटलेखिक) को क्रिप्टोग्राफिक (कूटलेख) सुरक्षा प्रणालियों को हटाने और एन्क्रिप्टेड (कूटित) संदेशों की सामग्री तक पहुंच प्राप्त करने के लिए प्रयोग किया जाता है, भले ही क्रिप्टोग्राफिक (कूटलेख) कुंजी अज्ञात हो।

वास्तव में क्रिप्टैनालिसिस (कूटविश्लेषण) एन्क्रिप्टेड डेटा (कूटित आँकड़ा) को कुंजी के उपयोग के बिना अनएन्क्रिप्ट (unencrypt) या अकूटित करने का प्रयास है। क्रिप्टोग्राफी (कूटलेखन) का दूसरा पक्ष, क्रिप्टैनालिसिस (कूटविश्लेषण) के उपयोग से कमजोरियों को ढूंढकर कोड (कूट) तोड़ने के लिए किया जाता है। खराब उद्देश्यों वाले हैकर्स (hackers) द्वारा उपयोग किए जाने के अतिरिक्त, क्रिप्टैनालिसिस (कूटविश्लेषण) का प्रयोग अक्सर सेना द्वारा किया जाता है।

1.3 क्रिप्टोलॉजी (कूटलिपि):

क्रिप्टोलॉजी (कूटलिपि) गुप्त संदेश के कोडिंग (कोडन) और डिकोडिंग (अकोडन) का विज्ञान है। इसे क्रिप्टोग्राफी (कूटलेखन) में बांटा जाता है, जो क्रिप्टोसिस्टम (कूटतंत्र) और क्रिप्टैनालिसिस (कूटविश्लेषण) की अभिकल्पना करने से संबंधित है, और जो क्रिप्टोसिस्टम (कूटतंत्र) को तोड़ने से संबंधित है। क्रिप्टोलॉजी (कूटलिपि), कोडित संदेशों का अध्ययन, लगभग 1900 ईसा पूर्व मिस्र में माना जा सकता है, जब एक लेखक ने खनुमोतप द्वितीय के मकबरे में एक चट्टान में कुछ हाइरोग्लिफिक (hieroglyphic) प्रतीकों का निर्माण किया था। क्रिप्टोलॉजी (कूटलिपि) तब मुश्किल नहीं थी, क्योंकि ज्यादातर लोग अशिक्षित थे और केवल अभिजात वर्ग किसी भी लिखित भाषा को पढ़ सकते थे। फिरौन और शक्तिशाली, राजा और रानियां, राष्ट्रपति और तानाशाह, और सैन्य कमांडरों ने तब से अपने दुश्मनों से अपने संचार छिपाने के लिए क्रिप्टोलॉजी (कूटलिपि) का उपयोग किया है।

शब्द क्रिप्टोलॉजी (कूटलिपि) की उत्पत्ति प्राचीन ग्रीक में हुई है। यह दो घटकों से बना है, क्रिप्टोस (kryptos), जिसका अर्थ छुपा हुआ है, और लोगो (logos) जिसका अर्थ शब्द है। क्रिप्टोलॉजी (कूटलिपि) को लेखन के रूप में पुराना माना जाता है, और सांकेतिक भाषा को क्रिप्टोलॉजी (कूटलिपि) का सबसे पुराना रूप माना जा सकता है। सभ्यता की शुरुआत से बड़े पैमाने पर इलेक्ट्रॉनिक संचार के आगमन से, क्रिप्टोलॉजी (कूटलिपि) का मुख्य रूप से सैन्य और राजनयिक संचार की रक्षा के लिए उपयोग किया गया था। तब से यह आम आदमी के संचार का भी हिस्सा बन गया है क्योंकि अधिक से अधिक लोग ई–मेल जैसे इलेक्ट्रॉनिक संचार में बदल रहे हैं। उदाहरण के लिए, अतीत में, युद्ध के दौरान सेना द्वारा क्रिप्टोलॉजी (कूटलिपि) का उपयोग यह सुनिश्चित करने के लिए किया जाता था कि रणनीतियों को विरोधियों के लिए प्रकट नहीं किया गया था।

क्रिप्टोलॉजी (कूटलिपि), डेटा (आँकड़ा) संचार और भंडारण को आमतौर पर गुप्त रूप में सुरक्षित रखने से संबंधित विज्ञान है। इसमें क्रिप्टोग्राफी (कूटलेखन) और क्रिप्टैनालिसिस (कूटविश्लेषण) दोनों शामिल हैं। सुरक्षा वैध उपयोगकर्ताओं से प्राप्त होती है जो एक गुप्त कुंजी या कुंजी के आधार पर जानकारी को परिवर्तित करने में सक्षम होती है। परिणामी सिफर (कूटलेख), हालांकि गुप्त कुंजी के बिना आम तौर पर अचूक और ज्ञात योग्य नहीं है। छिपी हुई जानकारी को पुनर्प्राप्त करने या स्रोत को प्रमाणीकृत करने के लिए कुंजी को जानने वाले किसी भी व्यक्ति द्वारा डिक्रिप्ट (अकूटित) किया जा सकता है। गुप्तता, हालांकि क्रिप्टोलॉजी (कूटलिपि) में अभी भी एक महत्वपूर्ण कार्य है, अक्सर परिवर्तन का उपयोग करने का मुख्य उद्देश्य नहीं होता है, और परिणामी परिवर्तन केवल एक सिफर (कूटलेख) माना जा सकता है।

1.4 स्टेग्नोग्राफी (गुप्त लेखन):

स्टेग्नोग्राफी (गुप्त लेखन), क्रिप्टोग्राफी (कूटलेखन) के ही समान है लेकिन यह इसमें एक और आयाम जोड़ता है। इस विधि में, व्यक्ति न केवल छुपाकर जानकारी की गोपनीयता की रक्षा करना चाहते हैं, बल्कि वे यह भी सुनिश्चित करना चाहते हैं कि किसी भी अनाधिकृत व्यक्ति को ऐसी कोई पुष्टि न होने पाये कि कोई जानकारी भी उपलब्ध है। उदाहरण के लिए, अदृश्य वॉटरमार्किंग।

स्टेग्नोग्राफी (गुप्त लेखन) में, एक अवांछित व्यक्ति इस तथ्य से अनजान होता है कि देखे गए प्रेक्षित डेटा (आंकड़ा) में कौन सी जानकारी छिपी हुई है, जबकि क्रिप्टोग्राफी (कूटलेखन) में, अवांछित व्यक्ति को आम तौर पर यह पता होता है कि डेटा (आंकड़ा) को संप्रेषित किया जा रहा है, क्योंकि वे कोडेड संदेश देख सकते हैं।

स्टेग्नोग्राफी (गुप्त लेखन) एक फाइल, संदेश, छवि या वीडियो को किसी अन्य फाइल, संदेश, छवि या वीडियो के भीतर छिपाने का अभ्यास है। स्टेग्नोग्राफी (गुप्त लेखन) शब्द ग्रीक शब्द स्टेग्नोस (στεγανός) जिसका अर्थ है 'संरक्षित' और ग्रैफिन (γράφειν) जिसका अर्थ है 'लेखन' को जोड़ता है।

स्टेग्नोग्राफी (गुप्त लेखन) के पहले दस्तावेजी उपयोगों को 440 ईसा पूर्व में देखा जा सकता है जब हेरोडोटस ने अपने इतिहास में दो उदाहरणों का उल्लेख किया है। हिस्टियायू ने अपने सबसे भरोसेमंद नौकर के सिर का मुंडन करके उसपर संदेश चिह्नित करके अपने वासल, अरिस्टागोरास के पास भेजा था। इसके अतिरिक्त, डेमेट्रस ने मधुमक्खियों की सतह को लागू करने से पहले सीधे मोम टैबलेट की लकड़ी पर संदेश लिखकर ग्रीस पर होने वाले हमले के बारे में एक चेतावनी भेजी थी।

स्टेग्नोग्राफी (गुप्त लेखन) का एक और दस्तावेजी उपयोग 1499 में अपने स्टेग्नोग्राफिया (गुप्त लेख) में जोहान्स ट्रिथेमियस द्वारा किया गया था, जो क्रिप्टोग्राफी (कूटलेखन) और स्टेग्नोग्राफी (गुप्त लेखन) पर एक ग्रंथ था, जो जादू पर एक पुस्तक के रूप में छिपा हुआ था। आम तौर पर, छुपे हुए संदेश कुछ और (या इसका हिस्सा बनने के लिए) दिखाई देते हैंः जैसे छवियां, लेख या कुछ अन्य संरक्षित पाठ। उदाहरण के लिए, छुपा हुआ संदेश एक निजी पत्र की दृश्यमान रेखाओं के बीच अदृश्य स्याही में हो सकता है। स्टेग्नोग्राफिक (गुप्त लेखीय) योजनाएं केर्कहोफ के सिद्धांत का पालन करती हैं। क्रिप्टोग्राफी (कूटलेखन) पर स्टेग्नोग्राफी (गुप्त लेखन) का लाभ यह है कि इच्छित गुप्त संदेश स्वयं को जांच के उद्देश्य के रूप में ध्यान आकर्षित नहीं करता है। क्रिप्टोग्राफी (कूटलेखन) किसी संदेश की सामग्री की सुरक्षा का अभ्यास है, जबकि स्टेग्नोग्राफी (गुप्त लेखन) में एक गुप्त संदेश भेजा जाता है और साथ ही संदेश की सामग्री को भी छुपाया जाता है।

स्टेग्नोग्राफी (गुप्त लेखन) में कम्प्यूटर फाइल्स के अंदर जानकारी को छुपाना भी शामिल है। डिजिटल स्टेग्नोग्राफी (अंकीय गुप्त लेखन) में, इलेक्ट्रॉनिक संचार में एक परिवहन परत के अंदर स्टेग्नोग्राफिक (गुप्त लेखीय) कोडन शामिल हो सकता है, जैसे दस्तावेज फाइल, छवि फाइल, प्रोग्राम या प्रोटोकॉल। मीडिया फाइल्स अपने बड़े आकार के कारण स्टेग्नोग्राफिक (गुप्त लेखीय) संचार के लिए आदर्श है।

स्टेग्नोग्राफी (गुप्त लेखन) पृथक–पृथक, अदृश्य जानकारी के बिट्स के साथ नियमित कंप्यूटर फाइल्स (जैसे ग्राफिक्स, ध्वनि, टेक्स्ट, एचटीएमएल या फ्लॉपी डिस्क) में बेकार या अप्रयुक्त डेटा के बिट्स को प्रतिस्थापित करके काम करता है। यह छिपी हुई जानकारी प्लेन टेक्स्ट (साधारण पाठ), सिफर टेक्स्ट (कूटलेख पाठ) या यहां तक कि छवियां भी हो सकती है।

कभी–कभी स्टेग्नोग्राफी (गुप्त लेखन) का उपयोग तब किया जाता है जब एन्क्रिप्शन (कूट प्रक्रिया) की अनुमति नहीं है, या आमतौर पर, स्टेग्नोग्राफी (गुप्त लेखन) का उपयोग एन्क्रिप्शन (कूट प्रक्रिया) के पूरक के लिए किया जाता है। एक एन्क्रिप्टेड (कूटित) फाइल कभी भी स्टेग्नोग्राफी (गुप्त लेखन) का उपयोग करके जानकारी छिपा सकती है, इसलिए अगर एन्क्रिप्टेड (कूटित) फाइल को समझ लिया जाता है, तो भी छुपा संदेश नहीं देखा जाता है।

स्टेग्नोग्राफी (गुप्त लेखन) और क्रिप्टोग्राफी (कूटलेखन) के बीच का अंतर यह है कि क्रिप्टोग्राफी (कूटलेखन) में, कोई भी यह बता सकता है कि एक संदेश एन्क्रिप्ट (कूटित) किया गया है, लेकिन वह उचित कुंजी के ज्ञात हुए बिना संदेश को डीकोड (अकोडन) नहीं कर सकता है। स्टेग्नोग्राफी (गुप्त लेखन) में, संदेश को डीकोड (अकोडन) करना मुश्किल नहीं हो सकता है, लेकिन अधिकांश लोग संदेश की उपस्थिति का पता नहीं लगा पाते।

संयुक्त रूप में, स्टेग्नोग्राफी (गुप्त लेखन) और क्रिप्टोग्राफी (कूटलेखन) सुरक्षा के दो स्तर प्रदान कर सकती है। ऐसे कम्प्यूटर प्रोग्राम्स उपलब्ध हैं जो क्रिप्टोग्राफी (कूटलेखन) का उपयोग करके एक संदेश एन्क्रिप्ट (कूटित) करते हैं, और स्टेग्नोग्राफी (गुप्त लेखन) का उपयोग करके छवि के भीतर एन्क्रिप्शन (कूट प्रक्रिया) को छुपाते हैं।

1.5 क्रिप्टोग्राफी (कूटलेखन) का इतिहास :

क्रिप्टोग्राफी (कूटलेखन) की कला का जन्म लेखन की कला के साथ माना जा सकता है। जैसे–जैसे सभ्यताओं का विकास हुआ, जनजातियों, समूहों और साम्राज्यों में मनुष्यों का आयोजन हुआ। इससे लड़ाई, सर्वोच्चता और राजनीति जैसे विचारों का उदय हुआ। इन विचारों ने लोगों की प्राकृतिक आवश्यकता को चुनिंदा प्राप्तकर्ता के साथ गुप्त रूप से संवाद करने के लिए प्रेरित किया जिससे क्रिप्टोग्राफी का निरंतर विकास भी सुनिश्चित किया गया। क्रिप्टोग्राफी (कूटलेखन) की जड़ें रोमन और मिस्र की सभ्यताओं में पाई जाती हैं।

हाइरोग्लिफ – सबसे प्रथम क्रिप्टोग्राफिक (कूटलेखीय) तकनीकः

क्रिप्टोग्राफी (कूटलेखन) का प्रथम ज्ञात चिन्ह 'हाइरोग्लिफ' (hieroglyph) के उपयोग के लिए माना जा सकता है। लगभग 4000 साल पहले, मिस्र के लोग हाइरोग्लिफ में लिखे गए संदेशों से संवाद करते थे। यह कूट केवल उन शास्त्रीयों द्वारा जाना जाता था जो राजाओं की तरफ से संदेशों को प्रेषित करते थे।

बाद में, विद्वान 500 से 600 ईसा पूर्व के दौरान सरल मोनो–अल्फाबेटिक (mono-alphabetic) प्रतिस्थापन सिफर (कूटलेख) का उपयोग करने लगे। इसमें कुछ गुप्त नियमों के साथ संदेश के अक्षरों को अन्य अक्षरों के साथ प्रतिस्थापित करना शामिल था। यह नियम विकृत किए गए संदेश से मूल संदेश को पुनः प्राप्त करने की कुंजी बन गया।

क्रिप्टोग्राफी (कूटलेखन) की प्रथम रोमन विधि में, जिसे सीजर शिफ्ट सिफर (सीजर विस्थापन कूटलेख) के नाम से जाना जाता है, मूल संदेश के अक्षरों को एक सहमत संख्या पर स्थानांतरित करने पर निर्भर करता है, इस विकृत संदेश के अक्षरों को संदेश प्राप्तकर्ता द्वारा उसी संख्या से वापस पीछे की ओर स्थानांतरित कर मूल संदेश प्राप्त कर लिया जाता था।

1.5.1 क्रिप्टोग्राफी (कूटलेखन) का विकास :

यूरोपीय पुर्नजागरण के दौरान और उसके बाद, विभिन्न इतालवी और पापल राज्यों ने क्रिप्टोग्राफिक (कूटलेखीय) तकनीकों का तेजी से प्रसार किया। गुप्त कोड को तोड़ने के लिए इस युग में विभिन्न विश्लेषण तकनीकों का शोध किया गया था।

- 15वीं शताब्दी में विगनेर कोडिंग (Vigenere Coding) जैसी बेहतर कोडिंग तकनीकें अस्तित्व में आईं, जिसने संदेश में एक ही संख्या में स्थानांतरित करने के स्थान पर संदेश में कई अक्षरों के साथ संदेश ले जाने की पेशकश की।
- 19वीं शताब्दी के बाद, क्रिप्टोग्राफी एन्क्रिप्शन (कूटलेखन कूट प्रक्रिया) से अधिक परिष्कृत कला और सूचना सुरक्षा के विज्ञान के दृष्टिकोण से विकसित हुई।
- 20वीं शताब्दी की शुरुआत में, यांत्रिक और वैद्युतयांत्रिक मशीन जैसे अनिग्मा रोटर मशीन (Enigma Rotor Machine) के आविष्कार ने सूचना को कोड करने के अधिक उन्नत और कुशल साधन प्रदान किए।
- द्वितीय विश्व युद्ध की अवधि के दौरान, क्रिप्टोग्राफी (कूटलेखन) और क्रिप्टाएनालिसिस (कूटविश्लेषण) दोनों गणितीय बन गए।

इस क्षेत्र में होने वाली प्रगति के साथ, सरकारी संगठनों, सैन्य इकाइयों और कुछ व्यवसायिक घरानों ने क्रिप्टोग्राफी (कूटलेखन) के अनुप्रयोगों को अपनाना शुरू कर दिया। उन्होंने दूसरों से अपने भेदों की रक्षा के लिए क्रिप्टोग्राफी (कूटलेखन) का इस्तेमाल किया। वर्तमान में कंप्यूटर और इंटरनेट के आगमन ने प्रभावी क्रिप्टोग्राफी (कूटलेखन) की आम लोगों तक पहुंच को आसान बना दिया है।

1.5.2 प्राचीनकाल क्रिप्टोग्राफी (कूटलेखन):

क्रिप्टोग्राफी (कूटलेखन) की जड़ें 2000 बीसी के आसपास शुरू हुईं। मिस्र में जब मृतक के जीवन की कहानी बताने के लिए कब्र को सजाने के लिए हाइरोग्लिफिक्स का उपयोग किया जाता था। यह संदेशों को छिपाने के लिए नहीं था, लेकिन उन्हें अधिक महान, औपचारिक और राजसी दिखाने के लिए किया जाता था।

एन्क्रिप्शन (कूटित) विधियों को मुख्य रूप से दूसरों से जानकारी छिपाने के लिए उपयोग किए जाने वाले व्यावहारिक अनुप्रयोगों में दिखाने के लिए विकसित किया गया।

हिब्रू (Hebrew) क्रिप्टोग्राफिक (कूटलेखीय) विधि में वर्णमाला को व्यवस्थित करने की आवश्यकता होती है ताकि मूल वर्णमाला के प्रत्येक अक्षर को व्यवस्थित किए गए वर्णमाला के एक अलग अक्षर में प्रतिचित्रित किया जा सके। इस एन्क्रिप्शन (कूटित) विधि को *atbash* कहा जाता था। *atbash* एन्क्रिप्शन (कूटित) विधि में उपयोग की जाने वाली एन्क्रिप्शन (कूटित) कुंजी का एक उदाहरण निम्न प्रकार दिखाया गया है:

```
ABCDEFGHI JK LMNOPQ R STU VW XYZ
ZYXWVUTSR QP ONMLKJ I HGF ED CBA
```

उदाहरण के लिए, "security" शब्द को "hvxfirgb" में एन्क्रिप्ट (कूटित) किया गया है। इसी प्रकार "xrhhk" क्या होगा? यह एक प्रतिस्थापन सिफर (कूटलेख) है, क्योंकि एक कैरेक्टर (संप्रतीक) को दूसरे कैरेक्टर (संप्रतीक) के साथ प्रतिस्थापित कर दिया जाता है। इस प्रकार के प्रतिस्थापन सिफर (कूटलेख) को मोनोअल्फाबेटिक प्रतिस्थापन के रूप में भी जाना जाता है क्योंकि यह एक समय में एकाधिक वर्णमाला का उपयोग करने वाले अन्य सिफर (कूटलेख) की तुलना में केवल एक वर्णमाला का उपयोग करता है। इस सरल एन्क्रिप्शन (कूटित) विधि ने अपने समय और विशेष संस्कृतियों के लिए काम किया, लेकिन अंततः अधिक जटिल तंत्र की आवश्यकता थी।

लगभग 400 बीसी, स्पार्टन ने पपीरस की एक शीट (पर्ण) पर एक संदेश लिखकर जानकारी एन्क्रिप्ट (कूटित) करने की प्रणाली का उपयोग किया, जो एक बेलनाकार वस्तु के चारों ओर लपेटा गया था। (यह एक छड़ी या लकड़ी की छड़ी के चारों ओर लिपटे कागज के टुकड़े की तरह दिखता है।) संदेश केवल तभी पढ़ने योग्य था जब संदेश सही व्यक्ति के पास था, जिसे अक्षरों को ठीक तरह से मिलान करने की अनुमति थी। इसे स्किटल सिफर (कूटलेख) के रूप में जाना जाता है। जब बेलन से पर्ण को हटा दिया गया, तो लेखन केवल यादृच्छिक अक्षरों के एक गुच्छे के रूप में दिखाई देने लगा।

ग्रीक सरकार के वाहक सैनिकों के विभिन्न समूहों में पर्ण के इन टुकड़ों को चलाते थे। सैनिक तब सही व्यास और लंबाई के एक बेलन के चारों ओर पर्ण लपेटते थे और तब यादृच्छिक अक्षरों का मिलान होकर एक अर्थपूर्ण संदेश बन जाता था। इनका उपयोग सैनिकों को सामरिक चाल पर निर्देशित करने और उन्हें सैन्य निर्देश प्रदान करने के लिए किया जाता था।

इतिहास में एक अन्य समय और जगह में, जूलियस सीजर ने *atbash* विधि के समान वर्णमाला के अक्षरों को स्थानांतरित करने का एक सरल तरीका विकसित किया। आज यह तकनीक प्रभावी होने के लिए बहुत सरल लगती है, लेकिन उस समय बहुत से लोग नहीं पढ़ सकते थे, इसलिए यह उच्च स्तर की सुरक्षा प्रदान करता था।

1.5.3 मध्यकालीन क्रिप्टोग्राफी (कूटलेखन):

लगभग 1000 सीई, धर्म से कुरान का विश्लेषण करने के लिए प्रेरणा ने मोनोअल्फेबेटिक प्रतिस्थापन सिफर (कूटलेख) को तोड़ने के लिए आवृत्ति विश्लेषण तकनीक का आविष्कार किया। द्वितीय विश्व युद्ध तक यह सबसे मौलिक क्रिप्टैनालिटिक (कूटविश्लेषिक) अग्रिम था। 1465 में अल्बर्टी द्वारा पॉलीएल्फाबेटिक सिफर (कूटलेख) के आविष्कार तक सभी सिफर इस क्रिप्टैनालिटिक (कूटविश्लेषिक) तकनीक के लिए कमजोर बने रहे।

क्रिप्टैनालिसिस (कूटविश्लेषण) इस तथ्य का उपयोग करता है कि अधिकांश अंग्रेजी ग्रंथों में अक्षरों की आवृत्तियों बराबर नहीं होती है। उदाहरण के लिए, e, x से अधिक बार होता है।

राजनीतिक प्रतिस्पर्धा और धार्मिक क्रांति के परिणामस्वरूप क्रिप्टोग्राफी (कूटलेखन) महत्वपूर्ण हो गया। उदाहरण के लिए, पुनर्जागरण के दौरान और बाद में यूरोप में, विभिन्न इतालवी राज्यों के नागरिक, पापल राज्य और रोमन कैथोलिक चर्च क्रिप्टोग्राफिक (कूटलेखीय) तकनीकों की तेजी से वृद्धि के लिए जिम्मेदार थे, जिनमें से कुछ एल्बर्टी के अग्रिम को समझते हैं।

इस अवधि के दौरान विभिन्न प्रयोजनों में क्रिप्टोग्राफी (कूटलेखन) के व्यापक उपयोग ने उपयोगकर्ताओं को तहस–नहस कर दिया था। क्रिप्टैनालिसिस (कूटविश्लेषण) और गुप्त कूरियर विश्वासघात को बाबिंगटन साजिश में चित्रित किया गया है, जिसके कारण मैरी, क्वीन एलिजाबेथ आई को मारने के इरादे से स्कॉट्स की रानी का क्रोध हुआ। क्रिप्टोग्राफी (कूटलेखन) और इसका दुरुपयोग, साजिश में शामिल था, जिसने माताहारी के निष्पादन का नेतृत्व किया और 20 वीं शताब्दी की शुरुआत में ड्रेफस के दृढ़ विश्वास और कारावास की झुकाव का कारण बन गया।

संक्षेप में, अक्षर विश्लेषण की आवृत्ति कुछ सिफर पर लागू नहीं की जा सकती है। अर्नेस्ट विन्सेंट राइट द्वारा लिखी गई पुस्तक Gadsby जिसमें अक्षर e नहीं है। फ्रांसीसी में लिखे गए जॉर्ज पेरेक द्वारा La Disparition पुस्तक और भी प्रभावशाली है, जिसमें एक e नहीं है। इन दशाओं में, अक्षर आवृत्ति विश्लेषण गुप्त संदेश का अनावरण करने में विफल रहता है। अक्षर विश्लेषण की आवृत्ति के उपयोग के अतिरिक्त, इस अवधि में, क्रिप्टोग्राफी (कूटलेखन) दोनों सकारात्मक और नकारात्मक तरीकों से प्रयोग किया जाता था। कुछ दुरुपयोग ने उपयोगकर्ताओं को तबाह कर दिया था, जबकि कुछ सही तरीके से उपयोग करते थे, जिससे अनगिनत लाभ हुए थे।

1.5.4 1800 से द्वितीय विश्व युद्ध तक क्रिप्टोग्राफी (कूटलेखन):

यद्यपि क्रिप्टोग्राफी (कूटलेखन) का एक लंबा और जटिल इतिहास है, लेकिन 19वीं शताब्दी तक यह एन्क्रिप्शन (कूटित) या क्रिप्टैनालिसिस (क्रिप्टो सिस्टम में कमजोरियों को खोजने का विज्ञान) के विज्ञापन के दृष्टिकोण से कहीं ज्यादा कुछ नहीं हुआ। उत्तरार्द्ध के उदाहरणों में चार्ल्स बैबेज के क्रिमियन वार युग में पॉलीएल्फाबेटिक सिफर (कूटलेख) के गणितीय क्रिप्टैनालिसिस (कूटविश्लेषण) पर काम शामिल है, जिसे कुछ समय बाद प्रशिया फ्रेडरिक कासिस्की ने पुनः खोज लिया और प्रकाशित किया।

इस समय क्रिप्टोग्राफी (कूटलेखन) को समझना आम तौर पर अंगूठे के कड़े नियम का उदाहरण था। 19वीं शताब्दी के बाद, अगस्ते केर्कहॉफ के क्रिप्टोग्राफिक (कूटलेखीय) लेखन देखें। एडगर एलन पो ने 1840 के दशक में सिफर (कूटलेख) को हल करने के लिए व्यवस्थित विधियों का उपयोग किया। विशेष रूप से उन्होंने फिलाडेल्फिया पेपर अलेक्जेंडर के वीकली (एक्सप्रेस) मेसेंजर में अपनी क्षमताओं का विज्ञापन किया, सिफर (कूटलेख) के उपायों को आमंत्रित किया, जिसमें से उन्होंने लगभग सभी को हल करने के लिए आगे बढ़ने को कहा। उनकी सफलता ने कुछ महीनों तक सार्वजनिक हलचल पैदा कर दिया। बाद में उन्होंने क्रिप्टोग्राफी (कूटलेखन) की विधियों पर एक निबंध लिखा जो प्रथम विश्व युद्ध के दौरान जर्मन कोड और सिफर (कूटलेख) को तोड़ने का प्रयास करने वाले नवीन ब्रिटिश क्रिप्टैनालिस्ट्स (कूटविश्लेषक) के लिए एक परिचय के रूप में उपयोगी साबित हुआ।

1917 में, गिल्बर्ट वर्नम ने एक टेलिटेप सिफर (कूटलेख) का प्रस्ताव दिया जिसमें पेपर टेप पर एक पूर्व–तैयार कुंजी को रखकर, सिफर टेक्स्ट (कूटलेख पाठ) का उत्पादन करने के लिए प्लेन टेक्स्ट (साधारण पाठ) संदेश को कैरेक्टर (संप्रतीक) दर कैरेक्टर (संप्रतीक) संयुक्त किया जाता है। इससे वन टाइम पैड और इलेक्ट्रोमेक्निकल उपकरणों का उपयोग सिफर (कूटलेख) मशीनों के रूप में करने के विकास को बल मिला।

1932 में द्वितीय विश्व युद्ध से पहले की अवधि में गणितीय विधियां बढ़ीं (विशेष रूप से क्रिप्टैनालिसिस (कूटविश्लेषण) और सिफर (कूटलेख) विकास के लिए सांख्यिकीय तकनीकों के विलियम एफ. फ्राइडमैन अनुप्रयोग में और इनिग्मा प्रणाली के जर्मन सेना के संस्करण में मैरीन रेजेवेस्की के प्रारंभिक तोड़ में)। क्रिप्टोग्राफी (कूटलेखन) और क्रिप्टैनालिसिस (कूटविश्लेषण) दोनों द्वितीय विश्व युद्ध के बाद से कहीं अधिक गणितीय बन गए थे। इसके बाद भी, कम्प्यूटर्स की व्यापक उपलब्धता और संचार माध्यम के रूप में इंटरनेट होने के कारण, राष्ट्रीय सरकारों या इसी तरह के बड़े उद्यमों के अतिरिक्त किसी भी अन्य व्यक्ति के द्वारा क्रिप्टोग्राफी (कूटलेखन) का प्रभावी उपयोग किया जाने लगा।

द्वितीय विश्व युद्ध के समय, यांत्रिक और इलेक्ट्रोमेकैनिकल क्रिप्टोग्राफिक सिफर मशीनों का व्यापक उपयोग किया गया था, हालांकि अव्यवहारिक हस्त तंत्र का उपयोग जारी रखा गया था। इस अवधि में व्यावहारिक और गणितीय क्रिप्टोग्राफी (कूटलेखन) दोनों में विकास किया गया था।

जर्मनी ने इनिग्मा नामक इलेक्ट्रोमेकैनिकल रोटर आधारित सिफर सिस्टम (कूटलेख प्रणाली) का कई रूपों में भारी उपयोग किया। मैरियन रेजवेस्की ने 1932 में सैद्धांतिक गणित का उपयोग करके प्रारंभिक जर्मन सेना इनिग्मा प्रणाली के कोड तोड़ दिया। यह हजारों वर्षों में क्रिप्टैनालिसिस (कूटविश्लेषण) में सबसे बड़ी सफलता थी।

1940 के बाद ब्रिटिश और डच क्रिप्टोग्राफर्स (कूटविश्लेषक) के सहयोग से अमेरिकी नौसेना के क्रिप्टोग्राफर्स (कूटविश्लेषक) ने कई जापानी नौसेना क्रिप्टोसिस्टम (कूटतंत्र) में प्रवेश किया। उनमें से एक ने कोड को तोड़कर, जेएन –25, मशहूर रूप से मिडवे की लड़ाई में अमेरिकी जीत का नेतृत्व किया। एक अमेरिकी सेना समूह, एसआईएस, उच्चतम सुरक्षा जापानी राजनयिक सिफर सिस्टम (कूटलेख प्रणाली) को तोड़ने में कामयाब रहा, एक इलेक्ट्रोमेकैनिकल स्टेपिंग स्विच मशीन जिसे अमेरिकियों द्वारा बैंगनी कहा जाता था, द्वितीय विश्व युद्ध के आरंभ होने से भी पहले की थी। अमेरिकियों ने क्रिप्टैनालिसिस (कूटविश्लेषण) के परिणामस्वरूप गुप्त जानकारी का उल्लेख किया, शायद विशेष रूप से बैंगनी मशीन से। ब्रिटिश अंततः क्रिप्टैनालिसिस (कूटविश्लेषण) के परिणामस्वरूप खुफिया जानकारी के लिए 'अल्ट्रा' पर बस गए, विशेष रूप से विभिन्न इनिग्मास द्वारा दिए गए एनसिफर (enciphered) संदेश से। अल्ट्रा के लिए पहले ब्रिटिश शब्द 'बोनिफेस' था।

जर्मन सेना ने वन टाइम पैड में कई यांत्रिक प्रयास भी किए। ब्लेलेली पार्क ने उन्हें फिश सिफर (कूटलेख) तथा मैक्स न्यूमैन और उनके सहयोगियों को क्रिप्टैनालिसिस (कूटविश्लेषण) के साथ सहायता करने के लिए विश्व के पहले प्रोग्राम करने योग्य डिजिटल इलेक्ट्रॉनिक कम्प्यूटर, कोलोसस को अभिकल्पित करने के लिए तैनात किया। जर्मन विदेश कार्यालय ने 1919 में वन टाइम पैड का उपयोग करना शुरू किया।

जापानी विदेश कार्यालय ने स्थानीय रूप से विकसित इलेक्ट्रिकल स्टेपिंग स्विच आधारित प्रणाली का उपयोग किया, और कुछ जापानी दूतावासों में संलग्न करने के लिए कई समान मशीनों का भी उपयोग किया। इनमें से एक को अमेरिका द्वारा 'एम–मशीन' कहा जाता था, तथा एक अन्य को 'रेड' कहा जाता था। द्वितीय विश्व युद्ध में उपयोग की जाने वाली अन्य सिफर (कूटलेख) मशीनों में ब्रिटिश टाइपएक्स (TypeX) और अमेरिकन सिगबा (SIGABA) शामिल थे। दोनों इलेक्ट्रोमेक्निकल रोटर अभिकल्पना में इनिग्मा के समान थे।

संक्षेप में, प्रतिद्वंद्वियों की जानकारी को छिपाने के लिए विभिन्न सिफर (कूटलेख) मशीनों को नियोजित किया गया था। ये सिफर (कूटलेख) मशीन्स इलेक्ट्रोमैकेनिकल संचालित थीं, उदाहरण के लिए इलैग्मा, कोलोसस, बैंगनी, टाइपएक्स और सिगाबा आदि।

1.5.5 आधुनिक क्रिप्टोग्राफी (कूटलेखन):

आधुनिक क्रिप्टोग्राफी (कूटलेखन) कम्प्यूटर और संचार सुरक्षा की आधारशिला है। इसकी नींव गणित की विभिन्न अवधारणाओं पर आधारित है जैसे संख्या सिद्धांत, कम्प्यूटेशनल–जटिलता सिद्धांत, और संभाव्यता सिद्धांत।

आधुनिक क्रिप्टोग्राफी (कूटलेखन) का युग वास्तव में 1949 में क्लाउड शैनन के साथ शुरू होता है, जो कि गणितीय क्रिप्टोग्राफी (कूटलेखन) के पिता हैं। 1976 में, दो प्रमुख सार्वजनिक प्रगति हुई। प्रथम डीईएस (डेटा एन्क्रिप्शन मानक) [DES (Data Encryption Standard)] था। 1976 में दूसरा विकास शायद और भी महत्वपूर्ण था, क्योंकि मूल रूप से क्रिप्टोसिस्टम (कूटतंत्र) काम कर सकते थे। यह व्हाइटफील्ड डिफी और मार्टिन हेलमैन द्वारा क्रिप्टोग्राफी (कूटलेखन) में शोध पत्र का प्रकाशन था, जिसने क्रिप्टोग्राफी (कूटलेखन) को नई दिशा प्रदान की। इस शोध पत्र में क्रिप्टोग्राफिक (कूटलेखीय) कुंजी वितरित करने की एक नई विधि प्रस्तुत की गई, जो क्रिप्टोग्राफी (कूटलेखन) की कुंजी वितरण की मौलिक समस्याओं में से एक को हल करने के लिए थी, और इसे डिफी–हेलमैन कुंजी एक्सचेंज (Diffie-Hellman key exchange) के रूप में जाना जाने लगा।

संक्षेप में, इस अवधि के समय, कम्प्यूटर का क्रिप्टोग्राफिक (कूटलेखीय) उद्देश्यों में अत्यधिक उपयोग होने लगा, उदाहरण के लिए, डीईएस, 56–बिट आकार एन्क्रिप्शन। भले ही एन्क्रिप्शन आधारित कम्प्यूटर को आधुनिक और सुरक्षित माना जाता है, फिर भी यह ब्रूट फोर्स अटैक (brute force attack) से गुप्त संदेश की रक्षा करने के लिए अपर्याप्त है। परिणामतः, अग्रिम क्रिप्टोग्राफिक (कूटलेखीय) तकनीकों को कभी विकसित नहीं किया जा रहा है। हाल ही में, क्वांटम क्रिप्टोग्राफी (कूटलेखन) का प्रादुर्भाव हुआ है, जो उच्च क्षमता रखने के साथ–साथ सटीक रूप से जांच भी करता है। यह भविष्यवाणी कर सकता है कि क्वांटम प्रौद्योगिकियां वास्तविक अटूट क्रिप्टोग्राफी (कूटलेखन) का नया युग बन जाएंगी।

निम्न तीन प्रमुख विशेषताएं हैं जो आधुनिक क्रिप्टोग्राफी (कूटलेखन) को प्राचीन क्रिप्टोग्राफी (कूटलेखन) से पृथक करती हैं।

क्र0	प्रचीन क्रिप्टोग्राफी (कूटलेखन)	आधुनिक क्रिप्टोग्राफी (कूटलेखन)
1	यह परंपरागत कैरेक्टर्स (संप्रतीक), अर्थात् अक्षरों और अंकों को सीधे जोड़ता है।	यह बाइनरी बिट अनुक्रमों पर कार्य करता है।
2	यह मुख्य रूप से 'अस्पष्टता के माध्यम से सुरक्षा' पर आधारित है। कोडिंग के लिए नियोजित तकनीकों को गुप्त रखा जाता था और केवल संचार में संलग्न व्यक्ति ही उनके बारे में जान सकते थे।	यह सूचना की कोडिंग के लिए सार्वजनिक रूप से ज्ञात गणितीय एल्गोरिथम (कलन विधि) पर निर्भर करता है। गोपनीयता को एक सुरक्षित कुंजी के माध्यम से प्राप्त किया जाता है जिसे एल्गोरिथम (कलन विधि) के लिए बीज के रूप में उपयोग किया जाता है। एल्गोरिथम (कलन विधि) की अभिकलन कठिनाई, गुप्त कुंजी की अनुपस्थिति इत्यादि, हमलावर के लिए मूल जानकारी प्राप्त करने के लिए असंभव बनाते हैं, भले ही वह कोडिंग के लिए उपयोग किए गए एल्गोरिथम (कलन विधि) को जानता हो।
3	गोपनीय रूप से संचार करने के लिए इसमें संपूर्ण क्रिप्टोसिस्टम (कूटतंत्र) की आवश्यकता है।	आधुनिक क्रिप्टोग्राफी (कूटलेखन) को केवल गुप्त कुंजी रखने के लिए सुरक्षित संचार में संलग्न रहने वाले व्यक्तियों की आवश्यकता होती है।

1.6 क्रिप्टोग्राफी (कूटलेखन) का संदर्भः

क्रिप्टोलॉजी (कूटलिपि), क्रिप्टोसिस्टम (कूटतंत्र) का अध्ययन, दो शाखाओं में विभाजित किया जा सकता है –

- क्रिप्टोग्राफी (कूटलेखन)
- क्रिप्टएनालिसिस (कूटविश्लेषण)

क्रिप्टोग्राफी (कूटलेखन) क्या है?

क्रिप्टोग्राफी (कूटलेखन) एक क्रिप्टोसिस्टम (कूटतंत्र) बनाने की कला और विज्ञान है जो सूचना सुरक्षा प्रदान करने में सक्षम है।

क्रिप्टोग्राफी (कूटलेखन) डिजिटल डेटा (अंकीय आँकड़ा) की वास्तविक सुरक्षा के साथ संबंधित है। यह गणितीय एल्गोरिथम (कलन विधि) के आधार पर तंत्र के डिजाइन को संदर्भित करता है जो मौलिक सूचना सुरक्षा सेवाएं प्रदान करता है। हम गुप्त अनुप्रयोगों में विभिन्न तकनीकों वाली एक बड़ी टूलकिट की स्थापना के रूप में क्रिप्टोग्राफी (कूटलेखन) के बारे में सोच सकते हैं।

क्रिप्टैनालिसिस (कूटविश्लेषण) क्या है?

सिफर टेक्स्ट (कूटलेख पाठ) को तोड़ने की कला और विज्ञान को क्रिप्टैनालिसिस (कूटविश्लेषण) कहा जाता है। क्रिप्टैनालिसिस (कूटविश्लेषण) क्रिप्टोग्राफी (कूटलेखन) की एक सहयोगी शाखा है और वे दोनों सह–अस्तित्व में हैं। क्रिप्टोग्राफिक (कूटलेखीय) प्रक्रिया के परिणामस्वरूप संचरण या भंडारण के लिए सिफर टेक्स्ट (कूटलेख पाठ) में परिणाम प्राप्त होता है। इसमें क्रिप्टोग्राफिक (कूटलेखीय) तंत्र का अध्ययन उन्हें तोड़ने के लिए होता है। क्रिप्टैनालिसिस (कूटविश्लेषण) का उपयोग अपनी सुरक्षा शक्तियों का परीक्षण करने के लिए नई क्रिप्टोग्राफिक (कूटलेखीय) तकनीकों के डिजाइन के दौरान भी किया जाता है।

टीपः

क्रिप्टोग्राफी (कूटलेखन), क्रिप्टोसिस्टम (कूटतंत्र) की अभिकल्पना के साथ संबंधित है, जबकि क्रिप्टैनालिसिस (कूटविश्लेषण) क्रिप्टोसिस्टम (कूटतंत्र) के टूटने का अध्ययन करता है।

1.7 क्रिप्टोग्राफी (कूटलेखन) की सुरक्षा सेवायें:

क्रिप्टोग्राफी (कूटलेखन) के उपयोग करने का प्राथमिक उद्देश्य निम्नलिखित चार मौलिक सूचना सुरक्षा सेवाएं प्रदान करना है। हम क्रिप्टोग्राफी (कूटलेखन) द्वारा पूर्ण किए जाने वाले संभावित लक्ष्यों को देखेंगे।

1. गोपनीयताः

गोपनीयता क्रिप्टोग्राफी (कूटलेखन) द्वारा प्रदान की जाने वाली मौलिक सुरक्षा सेवा है। यह एक सुरक्षा सेवा है जो सूचना को अनाधिकृत व्यक्ति से दूर रखती है। इसे कभी–कभी गोपनीयता या गुप्तता के रूप में जाना जाता है। डेटा एन्क्रिप्शन के लिए गणितीय एल्गोरिथम (कलनविधि) के उपयोग से भौतिक सुरक्षा से शुरू होने वाले कई माध्यमों से गोपनीयता प्राप्त की जा सकती है।

2. डेटा अखंडताः

वह सुरक्षा सेवा जो डेटा में किसी भी परिवर्तन के पहचान करने से संबंधित होता है डेटा अखंडता कहलाता है। डेटा जानबूझकर या आकस्मिक रूप से एक अनाधिकृत इकाई द्वारा संशोधित किया जा सकता है। डेटा अखंडता डेटा के परिवर्तन को रोक नहीं सकती है, लेकिन यह पता लगाने के लिए एक साधन प्रदान करती है कि डेटा को अनधिकृत तरीके से छेड़छाड़ किया गया है या नहीं।

3. प्रमाणीकरणः

प्रमाणीकरण उत्प्रेरक की पहचान प्रदान करता है। यह प्राप्तकर्ता को यह पुष्टि करता है कि प्राप्त डेटा केवल एक पहचान और सत्यापित प्रेषक द्वारा भेजा गया है। प्रमाणीकरण सेवा के दो प्रकार हैं –

- **संदेश प्रमाणीकरणः** संदेश भेजने वाले राउटर या प्रधाली के बिना संदेश के उत्प्रेरक की पहचान करता है।
- **इकाई प्रमाणीकरणः** आश्वासन देता है कि किसी विशेष इकाई से डेटा (आँकड़ा) प्राप्त किया गया है, जैसे एक विशेष वेबसाइट से।

उत्प्रेरक के अतिरिक्त, प्रमाणीकरण सृजन/संचरण की तारीख और समय जैसे डेटा (आँकड़ा) से संबंधित अन्य मानकों के बारे में भी आश्वासन प्रदान कर सकता है।

4. अ–परित्यागः

यह एक सुरक्षा सेवा है जो सुनिश्चित करता है कि एक इकाई पिछली प्रतिबद्धता या कार्यवाही के स्वामित्व से इनकार नहीं कर सकती है। यह एक आश्वासन है कि डेटा (आँकड़ा) का मूल सृजनकर्ता किसी प्राप्तकर्ता या तृतीय पक्ष को उस डेटा (आँकड़ा) के सृजन या संचरण से इनकार नहीं कर सकता है।

अ–परित्याग एक ऐसी संपत्ति है जो उन परिस्थितियों में सबसे वांछनीय है जहां डेटा (आँकड़ा) के आदान–प्रदान पर विवाद की संभावना है। उदाहरण के लिए, यदि कोई आदेश इलेक्ट्रॉनिक रूप से किया जाता है, तो एक क्रेता क्रय आदेश से इन्कार नहीं कर सकता है, अगर इस लेनदेन में अ–परित्याग सेवा जोड़ी गई हो।

1.8 क्रिप्टोग्राफी (कूटलेखन) प्राथिमिकी:

क्रिप्टोग्राफी (कूटलेखन) प्राथिमिकी क्रिप्टोग्राफी (कूटलेखन) में उपकरण और तकनीकों के अतिरिक्त कुछ भी नहीं हैं जिन्हें चयनित सुरक्षा सेवाओं का एक समूह प्रदान करने के लिए वांछित रूप से उपयोग किया जा सकता है –

- एन्क्रिप्शन (कूट प्रक्रिया)
- हैश फंक्शन (द्रुतान्वेषण फलन)
- संदेश प्रमाणीकरण कोड (MAC)
- डिजीटल सिग्नेचर (अंकीय चिह्नक)

निम्नलिखित तालिका उन प्राथिमिकताओं को दिखाती है जो स्वयं को एक विशेष सुरक्षा सेवा प्रदान कर सकती हैं।

प्राथिमिकी → सेवायें ↓	**एन्क्रिप्शन (कूट प्रक्रिया)**	**हैश फंक्शन (द्रुतान्वेषण फलन)**	**संदेश प्रमाणीकरण कोड**	**डिजीटल सिग्नेचर (अंकीय चिह्नक)**
गोपनीयता	हाँ	नहीं	नहीं	नहीं
अखंडता	नहीं	कभी–कभी	हाँ	हाँ
प्रमाणीकरण	नहीं	नहीं	हाँ	हाँ
अ–परित्याग	नहीं	नहीं	कभी–कभी	हाँ

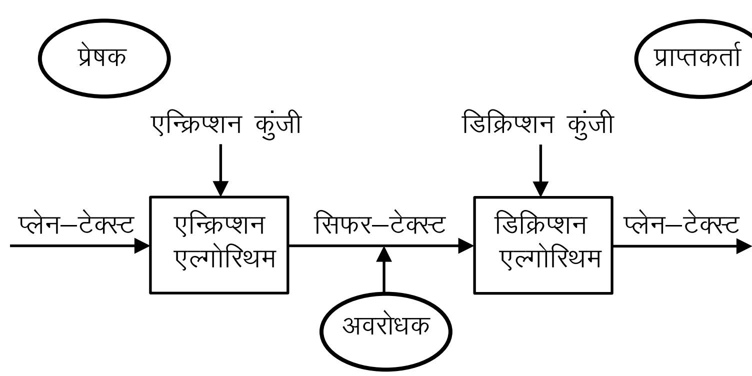
टीपः

क्रिप्टोग्राफिक (कूटलेखीय) प्राथिमिकी जटिल रूप से संबंधित हैं और उन्हें अक्सर क्रिप्टोसिस्टम (कूटतंत्र) से वांछित सुरक्षा सेवाओं के समूह को प्राप्त करने के लिए जोड़ा जाता है।

1.9 क्रिप्टोसिस्टम (कूटतंत्र):

क्रिप्टोसिस्टम (कूटतंत्र) सूचना सुरक्षा सेवाओं को प्रदान करने के लिए क्रिप्टोग्राफिक (कूटलेखीय) तकनीकों और उनके साथ–साथ बुनियादी ढांचे का कार्यान्वयन है। क्रिप्टोसिस्टम (कूटतंत्र) को सिफर (कूटलेख) प्रधाली भी कहा जाता है।

अब हम क्रिप्टोसिस्टम (कूटतंत्र) के एक सरल प्रारूप पर चर्चा करेंगे जो प्रसारित की जाने वाली सूचना को गोपनीयता प्रदान करता है। यह मूल प्रारूप नीचे दिए गए चित्र में चित्रित किया गया है –



(चित्र क्र0 1.2)

चित्रण एक प्रेषक को दिखाता है जो कुछ संवेदनशील डेटा को प्राप्तकर्ता की ओर इस प्रकार से स्थानांतरित करना चाहता है कि किसी भी अन्य व्यक्ति के द्वारा संचार प्रणाली पर अवरुद्ध या छेड़छाड़ करने से डेटा न निकाला जा सके।

इस सरल क्रिप्टोसिस्टम (कूटतंत्र) का उद्देश्य यह है कि प्रक्रिया के अंत में, केवल प्रेषक और प्राप्तकर्ता को प्लेन–टेक्स्ट (साधारण पाठ) ज्ञात होगा।

1.10 क्रिप्टोसिस्टम (कूटतंत्र) की शक्ति:

एन्क्रिप्शन (कूटित) विधि की शक्ति एल्गोरिथम (कलन विधि), कुंजी की गोपनीयता, कुंजी की लंबाई, प्रारंभिक सदिश और उनका एक साथ कार्य करना है। जब एन्क्रिप्शन (कूटित) में शक्ति पर चर्चा की जाती है, तो यह इंगित करता है कि एल्गोरिथम (कलन विधि) या कुंजी को समझना कितना मुश्किल है, जिसे सार्वजनिक नहीं किया जाता है। एक कुंजी को तोड़ना एक मान को खोजने की आशा में संभावित मानों की एक अद्भुत संख्या को संसाधित करना है, जिसका उपयोग किसी विशिष्ट संदेश को डिक्रिप्ट (अकूटित) करने के लिए किया जा सकता है। शक्ति, कुंजी प्रसंस्करण शक्ति और कुंजी को तोड़ने या कुंजी के मान को समझने में लगने वाले समय की मात्रा से संबंधित है। एक कुंजी को तोड़ने का अर्थ है कि परिणामस्वरूप प्लेन–टेकस्ट (साधारण–पाठ) प्राप्त होने तक हर संभव कुंजी मान का प्रयास किया रहा है। एल्गोरिथम (कलन विधि) और कुंजी की लंबाई के आधार पर, यह एक बहुत ही आसान कार्य या असंभव के करीब एक कार्य हो सकता है। यदि तीन घंटे में पेंटियम–2 प्रोसेसर के साथ एक कुंजी तोड़ी जा सकती है, तो सिफर (कूटलेख) बिल्कुल मजबूत नहीं है।

यदि कुंजी को केवल एक हजार मल्टीप्रोसेसिंग सिस्टम के उपयोग से तोड़ा जा सकता है, और इसमें 1.2 मिलियन वर्ष लगते हैं, तो यह बहुत मजबूत है। एक एन्क्रिप्शन (कूटित) विधि को अभिकल्पित करने का लक्ष्य अधिक समय लेने वाला होता है। क्रिप्टोग्राफी (कूटलेखन) शक्ति के लिए एक और नाम है कार्य कारक, जो एक हमलावर को एन्क्रिप्शन (कूटित) विधि में प्रवेश करने के प्रयास का आकलन है। सुरक्षा तंत्र की शक्ति एन्क्रिप्टेड डेटा (कूटित आँकड़ा) की संवेदनशीलता के साथ सहसंबंध में उपयोग की जानी चाहिए।

यहाँ तक कि अगर एल्गोरिथम (कलन विधि) बहुत जटिल और गहन है, तो एन्क्रिप्शन (कूटित) के अन्दर अन्य समस्याएँ हैं जो एन्क्रिप्शन (कूटित) विधियों की शक्ति को कमजोर कर सकती हैं। चूंकि कुंजी आमतौर पर संदेशों को एन्क्रिप्ट (कूटित) और डिक्रिप्ट (अकूटित) करने के लिए आवश्यक गुप्त मान होता है, इसलिए कुंजी की अनुचित सुरक्षा एन्क्रिप्शन (कूटित) शक्ति को कमजोर कर सकती है। एक बड़े कुंजीपटल का उपयोग करके एक बेहद मजबूत एल्गोरिथम (कलन विधि) का उपयोग किया जा सकता है, और एक बड़ा और यादृच्छिक कुंजी मान, जो मजबूत एन्क्रिप्शन (कूटित) के लिए आवश्यक है, लेकिन यदि कोई उपयोगकर्ता दूसरों के साथ अपनी कुंजी साझा करता है, तो समीकरण के अन्य टुकड़े वास्तव में काई अर्थ नहीं रखते हैं।

बिना किसी भी प्रकार की त्रुटियों के साथ एक एल्गोरिथम, एक वृहद् कुंजी, कुंजीपटल के अन्दर सभी संभावित मानों का उपयोग करके, वास्तविक कुंजी की रक्षा करना एन्क्रिप्शन (कूट प्रक्रिया) के महत्वपूर्ण तत्व हैं। यदि कोई कमजोर है, तो यह कमजोर संबंध साबित हो सकता है जो पूरी प्रक्रिया को प्रभावित करता है।

1.11 क्रिप्टोसिस्टम (कूटतंत्र) का लक्ष्य:

क्रिप्टोग्राफी (कूटलेखन) का लक्ष्य यह है कि दो व्यक्तियों के मध्य एक संदेश का आदान–प्रदान करना संभव हो ताकि अन्य व्यक्ति संदेश को न समझ सकें। इस प्रकार से किए जा सकने वाली विधियों का कोई अंत नहीं है। यहाँ हम टेक्स्ट (पाठ) को इस प्रकार परिवर्तित करने की विधियों से संबद्व होंगे कि प्राप्तकर्ता परिवर्तन को पूर्ववत कर सकता है और मूल टेक्स्ट (पाठ) को खोज सकता है।

मूल टेक्स्ट (पाठ) को आमतौर पर क्लीयर–टेक्स्ट (cleartext) कहा जाता है और एन्कोडेड या परिवर्तित टेक्स्ट को सिफर–टेक्स्ट (कूटलेख–पाठ) कहा जाता है। क्लीयर–टेक्स्ट से सिफर–टेक्स्ट में रूपांतरण को एन्कोडिंग या एन्सिफरिंग कहा जाता है, और विपरीत संक्रिया को डिकोडिंग या डिसिफरिंग कहा जाता है। यदि हम एक गुप्त संदेश पढ़ने की कोशिश कर रहे हैं जो हमारे लिए नहीं था और हम प्रारंभ में एन्कोडिंग विधि को नहीं जानते हैं, तो इस प्रक्रिया को कोड को क्रैकिंग करना कहा जाता है।

आम तौर पर, हमारे पास जितना अधिक सिफर–टेक्स्ट (कूटलेख–पाठ) होता है, कोड को तोड़ना उतना ही आसान होता है। अतः आमतौर पर कोडिंग तंत्र को नियमित रूप से बदलते रहना चाहिए। उदाहरण के लिए, यदि किसी कोडिंग योजना में कोई कीवर्ड होता है, और प्रत्येक दिन एक अलग कीवर्ड का उपयोग किया जाता है, तो संदेश को डीकोड करने के लिए पर्याप्त सिफर–टेक्स्ट (कूटलेख–पाठ) कभी नहीं हो सकता है। लेकिन यदि हम प्रत्येक दिन एन्कोडिंग बदलते हैं, तो हमारे पास नया कीवर्ड प्राप्त करने की एक सुरक्षित विधि होनी चाहिए।

क्रिप्टोसिस्टम (कूटतंत्र) गोपनीयता, प्रामाणिकता, अखंडता और अ–परित्याग सेवाएं प्रदान कर सकते हैं। यह डेटा या प्रणाली की उपलब्धता प्रदान नहीं करता है। गोपनीयता का मतलब है कि अनाधिकृत व्यक्ति जानकारी तक नहीं पहुंच सकते हैं। प्रामाणिकता संदेश के स्रोत को सत्यापित करने के लिए संदर्भित करती है ताकि प्रेषक को सही ढंग से पहचाना जा सके। ईमानदारी आश्वासन प्रदान करती है कि संदेश का संचार, गलती से या जानबूझकर संचार के समय संशोधित नहीं किया गया था। अ–परित्याग का अर्थ है कि एक प्रेषक बाद की तिथि में संदेश भेजने से मना नहीं कर सकता है, और प्राप्तकर्ता इसे प्राप्त करने से मना नहीं कर सकता है।

विभिन्न प्रकार के संदेशों और लेन–देन की एक या अधिक सेवाओं के लिए उच्च स्तर की आवश्यकता होती है जो एन्क्रिप्शन (कूटित) विधियों की आपूर्ति कर सकते हैं। सैन्य और खुफिया विभाग सूचना को गोपनीय रखने के बारे में अधिक चिंतित होते हैं, इसलिए वे एन्क्रिप्शन (कूटित) तंत्र चुनेंगे जो उच्च स्तर की गोपनीयता प्रदान करते हैं। वित्तीय संस्थान गोपनीयता के बारे में परवाह करते हैं, लेकिन प्रसारित होने वाले डेटा की अखंडता के बारे में अधिक परवाह करते हैं, इसलिए वे जो एन्क्रिप्शन (कूटित) तंत्र का चयन करते हैं। यह सेना के एन्क्रिप्शन (कूटित) विधियों से अलग हो सकता है।

1.11.1 क्रिप्टोसिस्टम (कूटतंत्र) के घटक:

एक मूल क्रिप्टोसिस्टम (कूटतंत्र) के विभिन्न घटक निम्नानुसार हैं –

प्लेन–टेक्स्ट (साधारण–पाठ): यह संचार के समय संरक्षित डेटा है।

एन्क्रिप्शन एल्गोरिथम (कूटित कलनविधि): यह एक गणितीय प्रक्रिया है जो किसी दिए गए प्लेन–टेक्स्ट (साधारण–पाठ) और एन्क्रिप्शन (कूटित) कुंजी के लिए एक सिफर–टेक्स्ट (कूटलेख–पाठ) जनित करता है। यह एक क्रिप्टोग्राफिक (कूटलेखीय) एल्गोरिथम (कलनविधि) है जो प्लेन–टेक्स्ट (साधारण–पाठ) और एन्क्रिप्शन (कूटित) कुंजी इनपुट (निवेश) के रूप में लेता है और एक सिफर–टेक्स्ट (कूटलेख–पाठ) उत्पन्न करता है।

सिफर–टेक्स्ट (कूटलेख–पाठ): यह एक विशिष्ट एन्क्रिप्शन (कूटित) कुंजी का उपयोग कर एन्क्रिप्शन एल्गोरिथम (कूटित कलनविधि) द्वारा जनित प्लेन–टेक्स्ट (साधारण–पाठ) का संकेतात्मक संस्करण है। सिफर–टेक्स्ट (कूटलेख–पाठ) की रक्षा नहीं की जाती है। यह सार्वजनिक प्रणाली पर रहता है। इसे किसी भी व्यक्ति द्वारा अवरुद्ध किया जा सकता है जिसके पास संचार प्रणाली तक पहुंच हो।

डिक्रिप्शन एल्गोरिदम (अकूटित कलनविधि): यह एक गणितीय प्रक्रिया है, जो किसी भी दिए गए सिफर–टेक्स्ट (कूटलेख–पाठ) और डिक्रिप्शन (अकूटित) कुंजी के लिए एक अद्वितीय प्लेन–टेक्स्ट (साधारण–पाठ) बनाता है। यह एक क्रिप्टोग्राफिक (कूटलेखीय) एल्गोरिथम (कलनविधि) है जो इनपुट (निवेश) के रूप में एक सिफर–टेक्स्ट (कूटलेख–पाठ) और डिक्रिप्शन (अकूटित) कुंजी लेता है, और एक प्लेन–टेक्स्ट (साधारण–पाठ) को आउटपुट के रूप में देता है। डिक्रिप्शन एल्गोरिथम (अकूटित कलनविधि) अनिवार्य रूप से एन्क्रिप्शन एल्गोरिथम (कूटित कलनविधि) को उलट देता है और इस प्रकार इससे निकटता से संबंधित होता है।

एन्क्रिप्शन (कूटित) कुंजी: यह एक मान है जो प्रेषक को ज्ञात होता है। प्रेषक सिफर–टेक्स्ट (कूटलेख–पाठ) की गणना करने के लिए प्लेन–टेक्स्ट (साधारण–पाठ) के साथ एन्क्रिप्शन एल्गोरिथम (कूटित कलनविधि) में एन्क्रिप्शन (कूटित) कुंजी इनपुट (निवेश) करता है।

डिक्रिप्शन (अकूटित) कुंजी: यह एक मान है जो प्राप्तकर्ता को ज्ञात होता है। डिक्रिप्शन (अकूटित) कुंजी एन्क्रिप्शन (कूटित) कुंजी से संबंधित है, लेकिन यह हमेशा समान नहीं होता है। प्लेन–टेक्स्ट (साधारण–पाठ) की गणना करने के लिए प्राप्तकर्ता सिफर–टेक्स्ट (कूटलेख–पाठ) के साथ डिक्रिप्शन एल्गोरिथम (अकूटित कलनविधि) में डिक्रिप्शन (अकूटित) कुंजी इनपुट (निवेश) करता है।

किसी दिए गए क्रिप्टोसिस्टम (कूटतंत्र) के लिए, सभी संभावित डिक्रिप्शन (अकूटित) कुंजियों का संग्रह एक की–स्पेस (key space) कहलात है।

अवरोधक: एक अनाधिकृत व्यक्ति जो प्लेन–टेक्स्ट (साधारण–पाठ) निर्धारित करने का प्रयास करता है। वह सिफर–टेक्स्ट (कूटलेख–पाठ) देख सकता है और डिक्रिप्शन एल्गोरिथम (अकूटित कलनविधि) को जान सकता है। हालांकि, उसे डिक्रिप्शन (अकूटित) कुंजी से कभी अवगत नहीं होना चाहिए।

1.11.2 क्रिप्टोसिस्टम (कूटतंत्र) के प्रकार:

मूल रूप से, दो प्रकार के क्रिप्टोसिस्टम (कूटतंत्र) होते हैं जिसकी सहायता से तंत्र में एन्क्रिप्शन–डिक्रिप्शन (कूटित–अकूटित) किया जाता है –

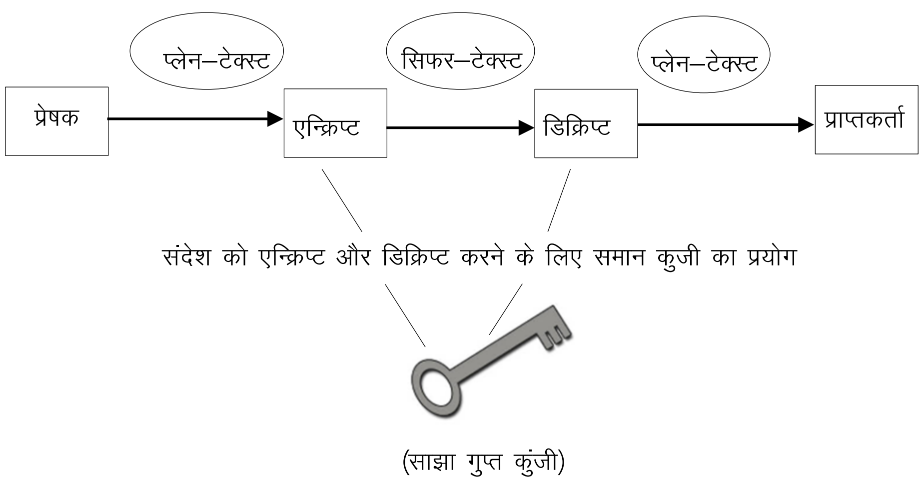
- सममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया)
- असममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया)

इन क्रिप्टोसिस्टम (कूटतंत्र) के मध्य मुख्य अंतर एन्क्रिप्शन और डिक्रिप्शन कुंजी के मध्य का संबंध है। तार्किक रूप से, किसी भी क्रिप्टोसिस्टम (कूटतंत्र) में, दोनों कुंजी निकटता से जुड़े होते हैं। एन्क्रिप्शन कुंजी से संबंधित कुंजी के साथ सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट करना व्यावहारिक रूप से असंभव है।

1.11.3 सममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया):

वह एन्क्रिप्शन प्रक्रिया जहाँ सूचना को एन्क्रिप्ट करने और डिक्रिप्ट करने के लिए समान कुंजी का उपयोग किया जाता है उसे सममित कुंजी एन्क्रिप्शन के रूप में जाना जाता है।

सममित क्रिप्टोसिस्टम (कूटतंत्र) का अध्ययन सममित क्रिप्टोग्राफी (कूटलेखन) के रूप में जाना जाता है। सममित क्रिप्टोसिस्टम (कूटतंत्र) को कभी–कभी गुप्त कुंजी क्रिप्टोसिस्टम (कूटतंत्र) के रूप में भी जाना जाता है। सममित कुंजी एन्क्रिप्शन विधियों के कुछ प्रसिद्ध उदाहरण हैं – डिजिटल एन्क्रिप्शन मानक (DES), त्रिक–डीईएस (Triple-DES), आईडीईए (IDEA) और ब्लोफिश (BLOWFISH)।



(चित्र क्र0 1.3)

1970 के पूर्व, सभी क्रिप्टोसिस्टम (कूटतंत्र) ने सममित कुंजी एन्क्रिप्शन को नियोजित किया था। आज भी, इसकी प्रासंगिकता बहुत अधिक है और इसका उपयोग कई क्रिप्टोसिस्टम (कूटतंत्र) में बड़े पैमाने पर किया जा रहा है। यह बहुत ही असंभव है कि यह एन्क्रिप्शन दूर हो जाएगा, क्योंकि इसमें असममित कुंजी एन्क्रिप्शन की तुलना में कुछ लाभ भी हैं।

सममित कुंजी एन्क्रिप्शन के आधार पर क्रिप्टोसिस्टम (कूटतंत्र) की मुख्य विशेषताएं निम्न हैं –

- सूचना के आदान–प्रदान से पहले सममित कुंजी एन्क्रिप्शन का उपयोग करने वाले व्यक्तियों को एक सामान्य कुंजी साझा करनी होगी।
- प्रणाली पर किसी भी हमले को रोकने के लिए नियमित रूप से सममित कुंजी बदलने की संस्तुत की जाती है।
- संचार पक्षों के मध्य कुंजी का आदान–प्रदान करने के लिए एक मजबूत तंत्र की आवश्यकता है। चूंकि कुंजी को नियमित रूप से बदला जाना आवश्यक है, इसलिए यह तंत्र खर्चीला और कष्टप्रद हो जाता है।
- n व्यक्तियों के एक समूह में, किन्हीं भी दो व्यक्तियों के मध्य दो–पक्षीय संचार को सक्षम करने हेतु समूह के लिए आवश्यक कुंजी की संख्या $n \times (n - 1)/2$ है।
- इस एन्क्रिप्शन में कुंजी की लंबाई (बिट्स की संख्या) छोटी होती है और इसलिए, एन्क्रिप्शन–डिक्रिप्शन की यह प्रक्रिया असममित कुंजी एन्क्रिप्शन की तुलना में तीव्र है।
- सममित एल्गोरिथम (कलनविधि) प्रक्रिया करने के लिए कम प्रक्रम शक्ति वाले कम्प्यूटर सिस्टम की आवश्यक होती है।

सममित कुंजी क्रिप्टोसिस्टम (कूटतंत्र) की चुनौतीः

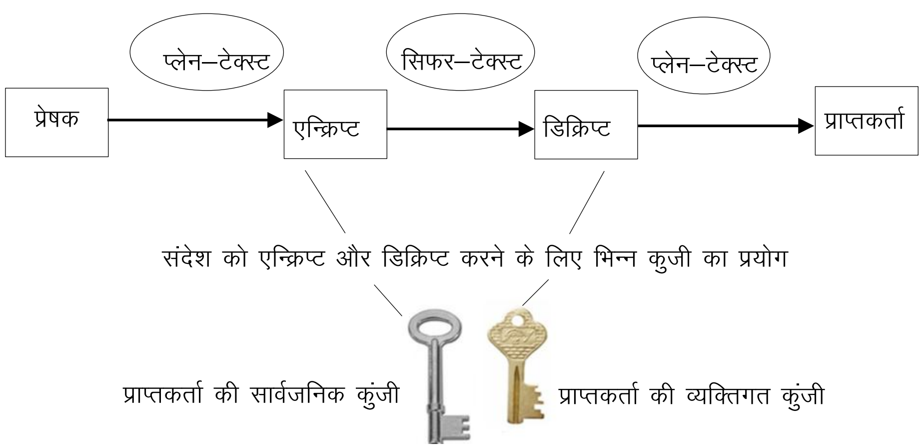
सममित कुंजी क्रिप्टोग्राफी (कूटलेखन) को नियोजित करने की दो प्रतिबंधित चुनौतियाँ हैं।

कुंजी की स्थापना: किसी भी संचार से पहले, प्रेषक और प्राप्तकर्ता दोनों को एक गुप्त सममित कुंजी पर सहमत होना चाहिए। इसके लिए एक सुरक्षित कुंजी स्थापना तंत्र की आवश्यकता है।

विश्वसनीयता: चूंकि प्रेषक और प्राप्तकर्ता एक ही सममित कुंजी का उपयोग करते हैं, इसलिए प्रेषक और प्राप्तकर्ता को एक दूसरे पर विश्वास करने की आवश्यकता होती है।

आधुनिक संचार के लिए ये दो चुनौतियां अत्यधिक प्रतिरोध उत्पन्न करती हैं। वर्तमान समय में व्यक्तियों को गैर–परिचित और गैर–भरोसेमंद के साथ सूचना का आदान–प्रदान करने की आवश्यकता होती है। उदाहरण के लिए, ऑनलाइन विक्रेता और ग्राहक के बीच एक संचार। सममित कुंजी एन्क्रिप्शन की इन सीमाओं ने असममित कुंजी एन्क्रिप्शन योजनाओं को जन्म दिया।

1.11.4 असममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया):



(चित्र क्र0 1.4)

एन्क्रिप्शन प्रक्रिया जहां सूचना को एन्क्रिप्ट करने और डिक्रिप्ट करने के लिए अलग–अलग कुंजियों का उपयोग किया जाता है, को असममित कुंजी एन्क्रिप्शन के रूप में जाना जाता है।

हालांकि कुंजियाँ अलग हैं, लेकिन वे गणितीय रूप से संबंधित हैं और इसलिए, सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट करके प्लेन–टेक्स्ट (साधारण–पाठ) को पुनर्प्राप्त करना संभव है।

व्यक्तियों के मध्य संचारण हेतु पूर्व–साझा गुप्त कुंजी को लाने के लिए 20वीं शताब्दी में असममित कुंजी एन्क्रिप्शन का आविष्कार किया गया। इस एन्क्रिप्शन योजना की मुख्य विशेषताएं निम्न हैं–

- इस प्रणाली के प्रत्येक उपयोगकर्ता को पृथक–पृथक व्यक्तिगत कुंजी और सार्वजनिक कुंजी की एक जोड़ी की आवश्यकता होती है। ये कुंजी गणितीय रूप से संबंधित हैं – जब एन्क्रिप्शन के लिए एक कुंजी का उपयोग किया जाता है, तो दूसरा सिफर–टेक्स्ट (कूटलेख–पाठ) को मूल प्लेन–टेक्स्ट (साधारण–पाठ) में वापस डिक्रिप्ट कर सकता है।
- इस विधि में सार्वजनिक कुंजी को सार्वजनिक संग्रह में रखने की आवश्यकता होती है और व्यक्तिगत कुंजी को गुप्त रूप में संरक्षित रखना होता है। इसलिए, एन्क्रिप्शन की इस योजना को सार्वजनिक कुंजी एन्क्रिप्शन भी कहा जाता है।
- हालांकि उपयोगकर्ता सार्वजनिक और व्यक्तिगत कुंजी से संबंधित हैं, लेकिन सार्वजनिक और व्यक्तिगत कुंजी को संगणन द्वारा एक दूसरे से प्राप्त नहीं किया जा सकता है। यही इस योजना की ताकत है।
- जब होस्ट 1 को होस्ट 2 पर डेटा भेजने की आवश्यकता होती है, तो वह सार्वजनिक संग्रह से होस्ट 2 की सार्वजनिक कुंजी प्राप्त करता है, डेटा को एन्क्रिप्ट करता है, और संचारित करता है।
- होस्ट 2 प्लेन–टेक्स्ट (साधारण–पाठ) प्राप्त करने के लिए अपनी व्यक्तिगत कुंजी का उपयोग करता है।
- इस एन्क्रिप्शन में कुंजी की लंबाई (बिट्स की संख्या) बड़ी है और इसलिए एन्क्रिप्शन–डिक्रिप्शन की यह प्रक्रिया सममित कुंजी एन्क्रिप्शन की तुलना में धीमी है।
- असममित एल्गोरिथम (कलनविधि) प्रक्रिया करने के लिए उच्च प्रक्रम शक्ति वाले कम्प्यूटर प्रणाली की आवश्यक होती है।

सममित क्रिप्टोसिस्टम (कूटतंत्र) एक प्राकृतिक अवधारणा है। इसके विपरीत, सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) को समझना काफी कठिन होता है।

1.12 सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) की चुनौती

सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) में एक महत्वपूर्ण चुनौती होती है। उपयोगकर्ता को इस बात का विश्वास करना पड़ता है कि एक सार्वजनिक कुंजी जिसे वह किसी दूसरे व्यक्ति के साथ संचार में उपयोग कर रहा है, वास्तव में उसी व्यक्ति की सार्वजनिक कुंजी है और किसी दुर्भावनापूर्ण तृतीय पक्ष द्वारा धोखा नहीं दिया गया है।

इसमें आमतौर पर एक सार्वजनिक कुंजी इंफ्रास्ट्रक्चर (PKI) के माध्यम से एक विश्वसनीय तृतीय पक्ष होता शामिल है। तृतीय पक्ष सार्वजनिक कुंजी की प्रामाणिकता को सुरक्षित रूप से प्रबंधित और प्रमाणित करता है। जब किसी तृतीय पक्ष से यह अनुरोध किया जाता है कि वह किसी भी संवाददाता व्यक्ति X के लिए सार्वजनिक कुंजी प्रदान करे, तो सही सार्वजनिक कुंजी प्राप्त करने के लिए विश्वास रखना होता है।

तृतीय पक्ष प्रमाणन या किसी अन्य प्रक्रिया द्वारा उपयोगकर्ता पहचान के बारे में खुद को संतुष्ट करता है कि X एकमात्र या वैश्विक रूप से अद्वितीय है। सत्यापित सार्वजनिक कुंजी उपलब्ध कराने के लिए सबसे सार्व विधि एक प्रमाणपत्र देना है जो विश्वसनीय तृतीय पक्ष द्वारा डिजिटल (अंकीय) हस्ताक्षरित हों।

दोनों प्रणालियों के लाभ और हानि के कारण, व्यावहारिक सूचना सुरक्षा प्रणालियों में सममित कुंजी और सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) का अक्सर एकसाथ उपयोग किया जाता है।

एन्क्रिप्शन योजनाओं के बीच संबंधः

दोनों प्रकार के क्रिप्टोसिस्टम (कूटतंत्र) के मूलभूत गुणों का सारांश नीचे दिया गया है –

	सममित क्रिप्टोसिस्टम (कूटतंत्र)	सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र)
कुंजीयों के मध्य संबंध	समान	भिन्न, लेकिन गणितीय रूप से संबंधित
एन्क्रिप्शन कुंजी	सममित	सार्वजनिक कुंजी
डिक्रिप्शन कुंजी	असममित	व्यक्तिगत कुंजी

1.13 क्रिप्टोसिस्टम (कूटतंत्र) के लिए केर्कहोफ का सिद्धांतः

19वीं शताब्दी में, एक डच क्रिप्टोग्राफर ए. केर्कहोफ ने एक अच्छे क्रिप्टोसिस्टम (कूटतंत्र) की आवश्यकताओं को प्रस्तुत किया। केर्कहोफ ने कहा कि एक क्रिप्टोग्राफिक निकाय सुरक्षित होना चाहिए, भले ही निकाय के बारे में सब कुछ, कुंजी को छोड़कर, सार्वजनिक ज्ञान हो। क्रिप्टोसिस्टम (कूटतंत्र) के लिए केर्कहॉफ ने छः अभिकल्पना सिद्धांत को परिभाषित किया है।

- क्रिप्टोसिस्टम (कूटतंत्र) को गणितीय रूप से नहीं, व्यावहारिक रूप से अटूट होना चाहिए।
- अनाधिकृत व्यक्ति के हाथों में क्रिप्टोसिस्टम (कूटतंत्र) को नहीं जाने देना चाहिए।
- कुंजी आसानी से प्रेषणीय, स्मरणार्थ और परिवर्तनीय होना चाहिए।
- सिफर–टेक्स्ट (कूटलेख–पाठ) टेलीग्राफ द्वारा संचारित होना चाहिए, एक असुरक्षित प्रणाली।
- एन्क्रिप्शन उपकरण और दस्तावेज एक व्यक्ति द्वारा वहनीय और संचालित होना चाहिए।
- अंत में, यह आवश्यक है कि निकाय का उपयोग करना आसान हो, न तो मानसिक तनाव और न ही नियमों की लंबी श्रृंखला के ज्ञान की आवश्यकता हो।

दूसरा नियम वर्तमान में केर्कहोफ सिद्धांत के रूप में जाना जाता है। यह लगभग सभी समकालीन एन्क्रिप्शन एल्गोरिथम (कूटित कलनविधि) में लागू होता है जैसे डीईएस (DES), एईएस (AES), आदि। इन सार्वजनिक एल्गोरिथम (कलनविधि) को पूरी तरह से सुरक्षित माना जाता है। एन्क्रिप्टेड संदेश की सुरक्षा पूरी तरह से गुप्त एन्क्रिप्शन कुंजी की सुरक्षा पर निर्भर करती है।

एल्गोरिथम (कलनविधि) को गोपनीय रखना क्रिप्टैनालिसिस (कूटविश्लेषण) के लिए एक महत्वपूर्ण बाधा के रूप में कार्य कर सकता है। हालांकि, एल्गोरिथम (कलनविधि) को गोपनीय रखना केवल तभी संभव होता है जब उनका सख्ती से सीमित परिधि में उपयोग किया जाता है।

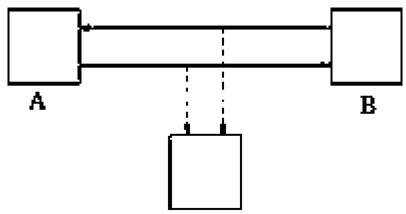
आधुनिक युग में, क्रिप्टोग्राफी (कूटलेखन) को उन उपयोगकर्ताओं को सेवा देने की आवश्यकता है जो इंटरनेट से जुड़े हुए हैं। इस दशा में, एक गोपनीय एल्गोरिथम (कलनविधि) का उपयोग करना संभव नहीं है, इसलिए आधुनिक क्रिप्टोग्राफी (कूटलेखन) में एल्गोरिथम (कलनविधि) अभिकलित करने के लिए केर्कहोफ सिद्धांत आवश्यक दिशा निर्देश बन गए।

1.14 क्रिप्टोसिस्टम (कूटतंत्र) पर आक्रमणः

वर्तमान समय में, न केवल व्यवसाय बल्कि मानव जीवन के लगभग सभी पहलुओं को सूचना द्वारा संचालित किया जाता है। इसलिए, आक्रमण जैसे दुर्भावनापूर्ण गतिविधियों से उपयोगी सूचना की रक्षा करना अनिवार्य हो गया है। अब हम सूचना पर होने वाले विभिन्न आक्रमण के प्रकारों पर विचार करेंगे जो आम तौर पर होते हैं। आक्रमणकर्त्ता द्वारा किए गए कार्यों के आधार पर आक्रमण को आम तौर पर वर्गीकृत किया जाता है। एक आक्रमण, इस प्रकार निष्क्रिय या सक्रिय हो सकता है।

निष्क्रिय आक्रमण :

निष्क्रिय आक्रमण का मुख्य लक्ष्य सूचना तक अनाधिकृत पहुंच प्राप्त करना है। उदाहरण के लिए, संचार प्रणाली पर अवरोधन और छिपाने जैसी कार्रवाइयों को निष्क्रिय आक्रमण के रूप में माना जा सकता है। एक निष्क्रिय आक्रमण सदैव सूचना चोरी के रूप में देखा जाता है।



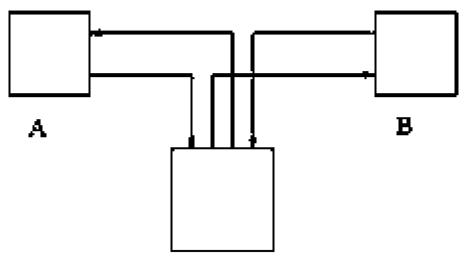
(निष्क्रिय आक्रमण)

(चित्र क्र0 1.5)

सक्रिय आक्रमण :

एक सक्रिय आक्रमण में सूचना पर कुछ प्रक्रिया आयोजित करके सूचना को किसी तरह से परिवर्तित करना शामिल है। उदाहरण के लिए:

- अनाधिकृत विधि से सूचना को संशोधित करना।
- सूचना के अनापेक्षित या अनाधिकृत संचरण की शुरुआत।
- प्रमाणीकृत डेटा (आंकड़ा) में परिवर्तन जैसे सूचना के साथ जुड़े जनक का नाम
- डेटा (आंकड़ा) को अनाधिकृत हटाना।
- वैध उपयोगकर्ताओं के लिए जानकारी तक पहुँचने से मना करना।



(सक्रिय आक्रमण)

(चित्र क्र0 1.6)

क्रिप्टोसिस्टम (कूटतंत्र) को लागू करने के लिए क्रिप्टोग्राफी (कूटलेखन) कई प्रकार के साधन और तकनीक प्रदान करता है जो ऊपर वर्णित अधिकांश आक्रमण को रोकने में सक्षम होता है।

सुरक्षा वातावरण:

क्रिप्टोसिस्टम (कूटतंत्र) पर होने वाले संभावित आक्रमण पर विचार करते समय, क्रिप्टोसिस्टम (कूटतंत्र) पर्यावरण को जानना आवश्यक है। पर्यावरण के बारे में आक्रमणकर्त्ता की धारणा और ज्ञान उसकी क्षमताओं से परिचित कराता है। क्रिप्टोग्राफी (कूटलेखन) में, सुरक्षा पर्यावरण और आक्रमणकर्त्ता की क्षमताओं के बारे में निम्नलिखित अवधारणायें हैं।

सार्वजनिक एल्गोरिथम (कलनविधि): इस विकल्प के साथ, एल्गोरिथम (कलनविधि) के सभी विवरण सार्वजनिक क्षेत्र में हैं, जिसे किसी भी व्यक्ति द्वारा जाना जा सकता है।

मालिकाना एल्गोरिथम (कलनविधि): एल्गोरिथम (कलनविधि) का विवरण केवल प्रणाली अभिकल्पना बनाने वाले और उपयोगकर्ताओं द्वारा जाना जाता है। मालिकाना एल्गोरिथम (कलनविधि) की दशा में, अस्पष्टता के माध्यम से सुरक्षा सुनिश्चित की जाती है। व्यक्तिगत एल्गोरिथम (कलनविधि) सबसे मजबूत एल्गोरिथम (कलनविधि) नहीं हो सकते हैं क्योंकि इन्हें घर में विकसित किया गया है और कमजोरी के लिए व्यापक रूप से जांच नहीं की जा सकती है।

द्वितीय, वे केवल बंद समूह के बीच संचार की अनुमति देते हैं। इसलिए वे आधुनिक संचार के लिए उपयुक्त नहीं हैं जहां लोग बड़ी संख्या में ज्ञात या अज्ञात संस्थाओं के साथ संवाद करते हैं। इसके अतिरिक्त, केर्कहॉफ के सिद्धांत के अनुसार, एल्गोरिथम (कलनविधि) को कुंजी में एन्क्रिप्शन की शक्ति के साथ सार्वजनिक होना पसंद किया जाता है।

इस प्रकार, सुरक्षा वातावरण के बारे में पहली धारणा यह है कि एन्क्रिप्शन एल्गोरिथम (कलनविधि) आक्रमणकर्त्ता को ज्ञात है।

सिफर–टेक्स्ट (कूटलेख–पाठ) की उपलब्धताः

हम जानते हैं कि जब प्लेन–टेक्स्ट (साधारण–पाठ) को सिफर–टेक्स्ट (कूटलेख–पाठ) में एन्क्रिप्ट (कूटित) किया जाता है, तब इसे संचार के लिए असुरक्षित सार्वजनिक प्रणाली पर रखा जाता है। इस प्रकार, आक्रमणकर्त्ता स्पष्ट रूप से यह मान सकता है कि क्रिप्टोसिस्टम (कूटतंत्र) द्वारा उत्पन्न सिफर–टेक्स्ट (कूटलेख–पाठ) तक पहुंच है।

प्लेन–टेक्स्ट (साधारण–पाठ) और सिफर–टेक्स्ट (कूटलेख–पाठ) की उपलब्धताः

यह धारणा अन्य के रूप में स्पष्ट नहीं है। हालांकि, ऐसी परिस्थितियां हो सकती हैं जहां आक्रमणकर्त्ता को प्लेन–टेक्स्ट (साधारण–पाठ) और संबंधित सिफर–टेक्स्ट (कूटलेख–पाठ) तक पहुंच हो सकती है। ऐसी कुछ संभावित परिस्थितियाँ हैं –

- आक्रमणकर्त्ता, प्रेषक को अपनी पसंद के प्लेन–टेक्स्ट (साधारण–पाठ) को परिवर्तित करने और सिफर–टेक्स्ट (कूटलेख–पाठ) प्राप्त करने पर प्रभाव डालता है।
- प्राप्तकर्ता असावधानी वश आक्रमणकर्त्ता को प्लेन–टेक्स्ट (साधारण–पाठ) प्रकट कर सकता है। आक्रमणकर्त्ता के पास खुली प्रणाली से एकत्रित संबंधित सिफर–टेक्स्ट (कूटलेख–पाठ) तक पहुंच है।
- एक सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) में, एन्क्रिप्शन कुंजी खुले क्षेत्र में होती है और किसी भी संभावित आक्रमणकर्त्ता द्वारा जाना जा सकता है। इस कुंजी का उपयोग करके, वह संबंधित प्लेन–टेक्स्ट (साधारण–पाठ) और सिफर–टेक्स्ट (कूटलेख–पाठ) का युग्म जनित कर सकता है।

1.15 क्रिप्टोग्राफिक (कूटलेखीय) आक्रमण:

आक्रमणकर्त्ता का मूलभूत प्रयोजन एक क्रिप्टोसिस्टम (कूटतंत्र) को तोड़ना और सिफर–टेक्स्ट (कूटलेख–पाठ) से प्लेन–टेक्स्ट (साधारण–पाठ) प्राप्त करना है। प्लेन–टेक्स्ट (साधारण–पाठ) प्राप्त करने के लिए, आक्रमणकर्त्ता को केवल गुप्त डिक्रिप्शन (अकूटित) कुंजी को खोजने की आवश्यकता होती है, क्योंकि एल्गोरिथम (कलनविधि) पहले से ही सार्वजनिक क्षेत्र में होता है।

इसलिए, वह क्रिप्टोसिस्टम (कूटतंत्र) में उपयोग की जाने वाली गुप्त कुंजी को खोजने के लिए अधिकतम प्रयास लागू करता है। एक बार जब आक्रमणकर्त्ता कुंजी निर्धारित करने में सक्षम हो जाता है, तो जिस निकाय पर आक्रमण किया जाता है उसे खंडित माना जाता है। उपयोग की जाने वाली पद्धति के आधार पर, क्रिप्टोसिस्टम (कूटतंत्र) पर आक्रमण को निम्नानुसार वर्गीकृत किया गया हैः

केवल सिफर–टेक्स्ट (कूटलेख–पाठ) आक्रमण (COA): इस विधि में, आक्रमणकर्त्ता के पास सिफर–टेक्स्ट (कूटलेख–पाठ) के समूह तक पहुंच उपलब्ध होता है। उसके पास प्लेन–टेक्स्ट (साधारण–पाठ) तक पहुंच नहीं होती है। COA सफल होता तब कहा जाता है जब प्लेन–टेक्स्ट (साधारण–पाठ) को सिफर–टेक्स्ट (कूटलेख–पाठ) के दिए गए समूह से निर्धारित किया जा सकता हो। कभी–कभी, इस आक्रमण से एन्क्रिप्शन कुंजी निर्धारित की जा सकती है। आधुनिक क्रिप्टोसिस्टम (कूटतंत्र) को COA आक्रमण के विपरीत संरक्षित किया जाता है।

ज्ञात प्लेनटेक्स्ट (साधारण–पाठ) आक्रमण (KPA): इस विधि में, आक्रमणकर्त्ता सिफर–टेक्स्ट (कूटलेख–पाठ) के कुछ भागों के लिए प्लेन–टेक्स्ट (साधारण–पाठ) जानता है। इस सूचना का उपयोग कर शेष सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट करता है। यह कुंजी या किसी अन्य विधि के माध्यम से निर्धारित किया जा सकता है। इस आक्रमण का सबसे अच्छा उदाहरण ब्लॉक सिफर के विरूद्व रैखिक क्रिप्टैनालिसिस (कूटविश्लेषण) है।

चुना गया प्लेनटेक्स्ट (साधारण–पाठ) आक्रमण (CPA): इस विधि में, आक्रमणकर्त्ता के पास अपनी पसंद का एन्क्रिप्टेड टेक्स्ट (कूटित पाठ) होता है। अतः वह अपनी पसंद का सिफर–टेक्स्ट (कूटलेख–पाठ) और प्लेन–टेक्स्ट (साधारण–पाठ) का युग्म रखता है। यह एन्क्रिप्शन कुंजी निर्धारित करने के कार्य को सरल बनाता है।

इस आक्रमण का एक उदाहरण ब्लॉक सिफर के साथ–साथ हैश फंक्शन (द्रुतान्वेषण फलन) के विरूद्व लागू क्रिप्टैनालिसिस (कूटविश्लेषण)है। एक लोकप्रिय सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) RSA चुने हुए प्लेन–टेक्स्ट (साधारण–पाठ) हमलों के लिए भेद्य है।

शब्दकोश हमला: इस आक्रमण के कई प्रकार हैं, जिनमें से सभी को 'शब्दकोश' में संकलित करना शामिल है। इस आक्रमण की सबसे सरल विधि में, आक्रमणकर्त्ता सिफर–टेक्स्ट (कूटलेख–पाठ) और संबंधित प्लेन–टेक्स्ट (साधारण–पाठ) का एक शब्दकोश बनाता है। भविष्य में, जब एक आक्रमणकर्त्ता को सिफर–टेक्स्ट (कूटलेख–पाठ) मिलता है, तो वह शब्दकोश को इसी प्लेन–टेक्स्ट (साधारण–पाठ) को खोजने के लिए संदर्भित करता है।

ब्रूट फोर्स अटैक: इस विधि में, आक्रमणकर्त्ता सभी संभावित कुंजी का प्रयास करके कुंजी निर्धारित करने का प्रयास करता है। यदि कुंजी 8 बिट लंबी है, तो संभव कुंजी की संख्या $2^8 = 256$ है। आक्रमणकर्त्ता सिफर–टेक्स्ट (कूटलेख–पाठ) और एल्गोरिथम (कलनविधि) जानता है, अब वह डिक्रिप्शन के लिए सभी 256 कुंजी एक–एक करके प्रयास करता है। यदि कुंजी लंबी है तो आक्रमण को पूरा करने का समय बहुत अधिक होगा।

जन्मदिन आक्रमण: यह आक्रमण ब्रूट–फोर्स तकनीक का एक रूप है। इसका उपयोग क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखीय द्रुतान्वेषण फलन) के विरूद्व किया जाता है। जब कक्षा में छात्रों को उनके जन्मदिन के बारे में पूछा जाता है, तो उत्तर 365 तिथियों में से एक है। आइए मान लें कि पहले छात्र का जन्मदिन 03 अगस्त है। फिर अगले छात्र को ढूंढने के लिए जिसका जन्मदिन 03 अगस्त है, हमें $1.25^{*}\sqrt{365} \approx 25$ छात्रों से पूछताछ करने की आवश्यकता है।

इसी प्रकार, यदि हैश फंक्शन (द्रुतान्वेषण फलन) 64 बिट हैश मान उत्पन्न करता है, तो संभव हैश मान 1.8×10^{19} हैं। विभिन्न इनपुट (निवेश) के लिए फंक्शन का बार–बार मूल्यांकन करके, उसी आउटपुट को लगभग 5.1×10^{9} यादृच्छिक इनपुट (निवेश) के बाद प्राप्त होने की उम्मीद है।

यदि आक्रमणकर्त्ता दो पृथक–पृथक इनपुट प्राप्त करने में सक्षम होता है जो समान हैश मान देते हैं, तो यह एक टक्कर है और हैश फंक्शन (द्रुतान्वेषण फलन) खंडित हुआ कहा जाता है।

मैन इन मिडिल आक्रमण (MIM): इस आक्रमण के लक्ष्य अधिकांशतः सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) हैं जहां संचार होने से पहले महत्वपूर्ण विनिमय शामिल होता है।

- माना A, B से संवाद करना चाहता है, इसलिए B से सार्वजनिक कुंजी का अनुरोध करता है।
- एक आक्रमणकर्त्ता इस अनुरोध को रोकता है और अपनी सार्वजनिक कुंजी भेजता है।
- इस प्रकार, A जो संदेश B के लिए भेजता है, आक्रमणकर्त्ता पढ़ने में सक्षम है।
- संचार बनाए रखने के लिए, आक्रमणकर्त्ता अपनी सार्वजनिक कुंजी के साथ पढ़ने के बाद डेटा को फिर से एन्क्रिप्ट (कूटित) करता है और B को भेजता है।
- आक्रमणकर्त्ता अपनी सार्वजनिक कुंजी को A की सार्वजनिक कुंजी के रूप में भेजता है ताकि B इसे ले सके जैसे कि वह इसे A से लेता।

साइड चैनल आक्रमण (SCA): इस प्रकार का आक्रमण किसी विशेष प्रकार के क्रिप्टोसिस्टम (कूटतंत्र) या एल्गोरिथम (कलनविधि) के विरूद्व नहीं है। यह आक्रमण क्रिप्टोसिस्टम (कूटतंत्र) के भौतिक कार्यान्वयन में कमजोरी का लाभ उठाने के लिए लागू किया गया है।

समय पर आक्रमण: आक्रमणकर्त्ता इस तथ्य का लाभ उठाते हैं कि विभिन्न संगणनाएँ प्रोसेसर पर गणना करने के लिए पृथक–पृथक समय लेती हैं। ऐसे समय को मापकर, प्रोसेसर की एक विशेष गणना के बारे में जानना संभव है। उदाहरण के लिए, यदि एन्क्रिप्शन में लंबा समय लगता है, तो यह इंगित करता है कि गुप्त कुंजी लंबी है।

शक्ति विश्लेषण आक्रमण: यह आक्रमण समय के आक्रमण के समान है। अंतर इतना है कि अंतर्निहित गणनाओं की प्रकृति के बारे में जानकारी प्राप्त करने के लिए विद्युत की खपत की मात्रा का उपयोग किया जाता है।

दोष विश्लेषण आक्रमण: इस आक्रमण में, क्रिप्टोसिस्टम (कूटतंत्र) की त्रुटियों का परीक्षण किया जाता है और आक्रमणकर्त्ता उपयोगी जानकारी के परिणामस्वरूप आउटपुट का अध्ययन करता है।

आक्रमण की व्यावहारिकताः

यहाँ वर्णित क्रिप्टोसिस्टम (कूटतंत्र) पर आक्रमण अत्यधिक अकादमिक हैं, क्योंकि उनमें से अधिकांश अकादमिक समुदाय से आते हैं। वास्तव में, कई अकादमिक आक्रमण में पर्यावरण के साथ–साथ आक्रमणकर्त्ता की क्षमताओं के बारे में काफी अवास्तविक मान्यताओं को शामिल किया गया है। उदाहरण के लिए, चुने गए सिफर–टेक्स्ट (कूटलेख–पाठ) आक्रमण में, आक्रमणकर्त्ता को चुने गए प्लेन–टेक्स्ट (साधारण–पाठ) और सिफर–टेक्स्ट (कूटलेख–पाठ) के युग्म की अव्यवहारिक संख्या की आवश्यकता होती है। यह व्यावहारिक रूप से पूरी तरह से नहीं हो सकता है।

1.16 क्रिप्टोग्राफी (कूटलेखन) गुण और दोषः

वर्तमान में, नेटवर्क (जालक्रम) वैश्विक हो गए हैं और सूचनाओं ने बिट्स और बाइट्स का डिजिटल रूप लिया है। गंभीर जानकारी अब कम्प्यूटर पर डिजिटल (अंकीय) रूप में संग्रहीत, संसाधित और प्रसारित हो जाती है और संचार प्रणाली खोलती है।

चूंकि सूचना की एक महत्वपूर्ण भूमिका है, इसलिए आक्रमणकर्त्ता कम्प्यूटर प्रणाली को लक्षित कर रहे हैं और संवेदनशील सूचनाओं को चुरा सकते हैं या महत्वपूर्ण सूचना प्रणाली को बाधित कर सकते हैं।

आधुनिक क्रिप्टोग्राफी (कूटलेखन) यह सुनिश्चित करने के लिए तकनीकों का एक ठोस समूह प्रदान करता है कि वैध उपयोगकर्ताओं की सूचना तक पहुंच सुनिश्चित करते समय आक्रमणकर्त्ता के दुर्भावनापूर्ण प्रयोजनों को विफल कर दिया जाए। अब हम क्रिप्टोग्राफी (कूटलेखन) की सीमाओं के साथ–साथ क्रिप्टोग्राफी (कूटलेखन) के भविष्य से प्राप्त लाभों पर चर्चा करेंगे।

क्रिप्टोग्राफी (कूटलेखन) के गुणः

क्रिप्टोग्राफी (कूटलेखन) एक आवश्यक सूचना सुरक्षा उपकरण है। यह सूचना सुरक्षा की चार सबसे मूलभूत सेवाएं प्रदान करता हैः

गोपनीयता – एन्क्रिप्शन तकनीक अनाधिकृत प्रकाशन और सूचना तक पहुँच से सूचना और संचार की रक्षा कर सकता है।

प्रमाणीकरण – MAC और डिजिटल (अंकीय) हस्ताक्षर जैसे क्रिप्टोग्राफिक (कूटलेखीय) तकनीक जालसाजी के विरूद्व सूचना की रक्षा कर सकती हैं।

डेटा इंटीग्रटी – क्रिप्टोग्राफिक (कूटलेखीय) हैश फंक्शन (द्रुतान्वेषण फलन) डेटा (आँकड़ा) अखंडता के बारे में उपयोगकर्ताओं को आश्वस्त करने में महत्वपूर्ण भूमिका निभा रहे हैं।

अपरित्याग – डिजिटल (अंकीय) हस्ताक्षर प्रेषक द्वारा प्रेषित संदेश से मना करने के कारण उत्पन्न होने वाले विवाद के विरूद्व सुरक्षा के लिए गैर–अस्वीकरण सेवा प्रदान करता है।

क्रिप्टोग्राफी (कूटलेखन) द्वारा दी गई इन सभी मौलिक सेवाओं ने कम्प्यूटर प्रणाली का उपयोग बेहद कुशल और प्रभावी तरीके से नेटवर्क (जालक्रम) पर व्यवसाय के आचरण को सक्षम किया है।

क्रिप्टोग्राफी (कूटलेखन) के दोषः

सूचना सुरक्षा के चार मौलिक तत्वों के अतिरिक्त, अन्य मामले भी हैं जो सूचना के प्रभावी उपयोग को प्रभावित करते हैंः

- दृढ़ता से एन्क्रिप्टेड, प्रामाणिक, और डिजिटल हस्ताक्षरित सूचना निर्णय लेने के एक महत्वपूर्ण समय पर एक वैध उपयोगकर्ता के लिए भी पहुँचना कठिन हो सकता है। नेटवर्क या कम्प्यूटर प्रणाली पर हमला किया जा सकता है और एक आक्रमणकर्त्ता द्वारा गैर–कार्यात्मक प्रदान किया जा सकता है।
- उच्च गुणवत्ता, सूचना सुरक्षा के मौलिक पक्षों में से एक, क्रिप्टोग्राफी (कूटलेखन) के उपयोग के माध्यम से सुनिश्चित नहीं किया जा सकता है। सेवा के मना करने या सूचना प्रणाली के पूर्ण टूटने जैसे खतरों से बचने के लिए अन्य विधियों की आवश्यकता है।
- चयनित अभिगम नियंत्रण की सूचना सुरक्षा की एक और मौलिक आवश्यकता भी क्रिप्टोग्राफी (कूटलेखन) के उपयोग के माध्यम से साधित नहीं की जा सकती है। इसके लिए प्रशासनिक नियंत्रण और प्रक्रियाओं का उपयोग करने की आवश्यकता है।

- प्रणाली, प्रोटोकॉल (संदेशाचार) और प्रक्रियाओं के निर्बल अभिकल्पना से प्राप्त जनित सूचनाओं की भेद्यता और और उस पर होने वाले आक्रमण के विरूद्व क्रिप्टोग्राफी (कूटलेखन) सुरक्षा नहीं करता है। इन्हें उचित अभिकल्पना और रक्षात्मक आधारभूत संरचना की स्थापना के माध्यम से तय करने की आवश्यकता है।
- क्रिप्टोग्राफी (कूटलेखन) पर लागत आती है। लागत समय और मुद्रा के पदों में होती है।
  - सूचना प्रसंस्करण में क्रिप्टोग्राफिक (कूटलेखीय) तकनीकों का योग करने में विलंब होता है।
  - सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) के उपयोग के लिए सुदृढ़ वित्तीय बजट की आवश्यकता वाले सार्वजनिक कुंजी बुनियादी ढांचे की स्थापना और रख–रखाव की आवश्यकता होती है।
- क्रिप्टोग्राफिक (कूटलेखीय) तकनीक की सुरक्षा गणितीय समस्याओं की संगणना कठिनाई पर आधारित है। ऐसी गणितीय समस्याओं को हल करने या संगणना शक्ति में वृद्धि करके कोई भी क्रिप्टोग्राफिक (कूटलेखीय) तकनीक को कमजोर कर सकता है।

1.17 क्रिप्टोग्राफी (कूटलेखन) के अनुप्रयोग:

गोपनीयता:

गोपनीयता क्रिप्टोग्राफी (कूटलेखन) का सबसे स्पष्ट अनुप्रयोग है। क्रिप्टोग्राफी (कूटलेखन) का उपयोग व्यक्तिगत रहने से सूचना को एन्क्रिप्ट (कूटित) करके गोपनीयता को लागू करने के लिए किया जा सकता है। किसी को इस व्यक्तिगत डेटा को पढ़ने के लिए पहले इसे डिक्रिप्ट (अकूटित) करना होगा।

प्रमाणीकरण:

प्रमाणीकरण एक प्रक्रिया है जिसके माध्यम से कोई निश्चित सूचना सिद्व और सत्यापित की जा सकती है। कभी–कभी किसी दस्तावेज की उत्पत्ति, प्रेषक की पहचान, दस्तावेज और समय पर हस्ताक्षर किए जाने वाले समय और दिनांक, कम्प्यूटर या उपयोगकर्ता की पहचान और इसी तरह की पुष्टि करना आवश्यक होता है।

डिजिटल (अंकीय) हस्ताक्षर:

डिजिटल (अंकीय) हस्ताक्षर एक क्रिप्टोग्राफिक (कूटलेखीय) माध्यम है जिसकी सहायता से इनमें से कई को सत्यापित किया जा सकता है। दस्तावेज का डिजिटल (अंकीय) हस्ताक्षर, दस्तावेज और हस्ताक्षरकर्ता की व्यक्तिगत कुंजी दोनों के आधार पर सूचना का एक भाग होता है।

डिजिटल (अंकीय) हस्ताक्षर और हाथ से लिखे हस्ताक्षर दोनों इस तथ्य पर आश्रित होते हैं कि एक ही हस्ताक्षर वाले दो लोगों को खोजना बहुत दुष्कर है। प्रत्येक व्यक्ति के साथ कुछ अद्वितीय जोड़कर डिजिटल (अंकीय) हस्ताक्षर की गणना करने के लिए सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) का उपयोग किया जाता है। जब किसी संदेश को एन्क्रिप्ट (कूटित) करने के लिए सार्वजनिक–कुंजी क्रिप्टोग्राफी (कूटलेखन) का उपयोग किया जाता है, तो प्रेषक इच्छित प्राप्तकर्ता की सार्वजनिक कुंजी के साथ संदेश को एन्क्रिप्ट करता है। जब डिजिटल हस्ताक्षर की गणना करने के लिए सार्वजनिक कुंजी क्रिप्टोग्राफी का उपयोग किया जाता है, तो प्रेषक दस्तावेज की डिजिटल फिंगरप्रिंट (अंकीय अंगुलछाप) को अपनी व्यक्तिगत कुंजी के साथ एन्क्रिप्ट (कूटित) करता है। हस्ताक्षरकर्ता की सार्वजनिक कुंजी तक पहुंचने वाला कोई भी व्यक्ति हस्ताक्षर की पुष्टि कर सकता है।

डिजिटल (अंकीय) लिफाफा:

डिजिटल (अंकीय) लिफाफे में गोपनीय–कुंजी क्रिप्टोग्राफी (कूटलेखन) और एन्क्रिप्टेड गोपनीय कुंजी का उपयोग करके एन्क्रिप्टेड संदेश रखा जाता है। जबकि डिजिटल (अंकीय) लिफाफे आमतौर पर गोपनीय कुंजी को एन्क्रिप्ट (कूटित) करने के लिए सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) का उपयोग करते हों, यह आवश्यक नहीं है।

न केवल डिजिटल (अंकीय) लिफाफे कुंजी प्रबंधन समस्या को हल करने में सहायता करते हैं, बल्कि वे सुरक्षा त्याग के बिना प्रदर्शन (संदेश डेटा के प्रत्यक्ष एन्क्रिप्शन के लिए सार्वजनिक कुंजी प्रणाली का उपयोग करने के सापेक्ष) को बढ़ाते हैं। डिजिटल (अंकीय) लिफाफा तकनीक कुंजी विनिमय की एक विधि है, लेकिन सभी प्रमुख विनिमय प्रोटोकॉल (संदेशाचार) डिजिटल लिफाफे का उपयोग नहीं करते हैं।

पहचानः

पहचान एक प्रक्रिया है जिसके माध्यम से कोई भी किसी व्यक्ति या इकाई की पहचान का पता लगा सकता है। हमारे दैनिक जीवन में, हम अपने परिवार के सदस्यों, दोस्तों और सहकर्मियों को उनके भौतिक गुणों, जैसे आवाज, चेहरे या अन्य विशेषताओं से पहचानते हैं। बॉयोमीट्रिक्स नामक इन विशेषताओं का उपयोग केवल विशेष हार्डवेयर वाले कम्प्यूटर नेटवर्क पर किया जा सकता है। नेटवर्क पर इकाइयाँ क्रिप्टोग्राफिक (कूटलेखीय) विधियों का उपयोग करके एक–दूसरे की पहचान भी कर सकती हैं।

संचरण में गोपनीयताः

संचारित सूचना को रूपान्तरित करने के लिए सबसे वर्तमान गोपनीयता प्रणाली संचरण के लिए व्यक्तिगत कुंजी प्रणाली का उपयोग करती है क्योंकि यह सबसे तेज विधि है जो उचित आश्वासन और निम्न उपरि के साथ संचालित होती है।

भंडारण में गोपनीयताः

भंडारण में गोपनीयता आमतौर पर एकल–कुंजी प्रणाली द्वारा रखी जाती है जहां उपयोगकर्ता सत्र के आरंभ में कम्प्यूटर की कुंजी प्रदान करता है, और प्रणाली सामान्य उपयोग के दौरान एन्क्रिप्शन और डिक्रिप्शन को संरक्षित रखता है।

1.18 क्रिप्टोग्राफी (कूटलेखन) का भविष्यः

इल्लिप्टिक कर्व क्रिप्टोग्राफी (अण्डाकार–वक्र कूटलेखन) (ECC) का आविष्कार पहले ही हो चुका है लेकिन इसके लाभ और हानि अभी तक पूरी तरह से समझ में नहीं आये हैं। ECC बहुत कम समय में एन्क्रिप्शन और डिक्रिप्शन करने की अनुमति देता है।

इस प्रकार यह समान सुरक्षा के साथ उच्च मात्रा में डेटा को पारित करने की इजाजत देता है। हालांकि, एन्क्रिप्शन के अन्य विधियों के रूप में, सरकारी, वाणिज्यिक और व्यक्तिगत उपयोग के लिए स्वीकार किए जाने से पहले ECC का भी परीक्षण और सिद्ध किया जाना चाहिए।

क्वांटम गणना नई घटना है। आधुनिक कंप्यूटर एक 'बिट' नामक बाइनरी प्रारूप का उपयोग करके डेटा संग्रहीत करते हैं जिसमें 1 या 0 संग्रहीत किया जा सकता है, जबकि एक क्वांटम कम्प्यूटर एक से अधिक अवस्थाओं की क्वांटम सुपरपोजिशन का उपयोग कर डेटा संग्रहित करता है। ये बहुक मान वाली अवस्थाएँ क्वांटम बिट्स या क्यूबिट्स में संग्रहीत होती हैं। यह परंपरागत ट्रांजिस्टर प्रोसेसर की तुलना में तीव्र गति से संख्याओं की गणना करने की अनुमति देता है।

क्वांटम कंप्यूटर की शक्ति को समझने के लिए, आरएसए–640 (RSA-640) पर विचार करें, 193 अंकों के साथ एक संख्या, जिसे 5 महीने की अवधि में अस्सी 2.2GHz कम्प्यूटर द्वारा गुणनखंडित किया जा सकता है, जबकि यही कार्य एक क्वांटम कंप्यूटर 17 सेकंड से भी कम समय में कर सकता है।

इन तथ्यों को ध्यान में रखते हुए, आधुनिक क्रिप्टोग्राफी को संगणना करने के लिए कठिन समस्याओं को देखना होगा या वर्तमान में आधुनिक क्रिप्टोग्राफी (कूटलेखन) द्वारा पेश किए गए लक्ष्यों को संग्रहित करने की पूरी नई तकनीकों को तैयार करना होगा।

अभ्यास

1. क्रिप्टोग्राफी (कूटलेखन) की उत्पत्ति की अवधारणा को स्पष्ट कीजिए।
2. क्रिप्टैनालिसिस (कूटविश्लेषण) से क्या समझते हैं?
3. क्रिप्टोलॉजी (कूटलिपि) को समझाइए।
4. स्टेग्नोग्राफी (गुप्त लेखन) क्या है?
5. क्रिप्टोग्राफी (कूटलेखन) का इतिहास संक्षेप में बताइए।
6. क्रिप्टोग्राफी (कूटलेखन) के विकास पर संक्षिप्त टिप्पणी लिखिए।

7. प्राचीनकाल क्रिप्टोग्राफी (कूटलेखन) पर टिप्पणी लिखिए।
8. मध्यकालीन क्रिप्टोग्राफी (कूटलेखन) से क्या समझते हैं?
9. 1800 से द्वितीय विश्व युद्व तक क्रिप्टोग्राफी (कूटलेखन) को समझाइए।
10. आधुनिक क्रिप्टोग्राफी (कूटलेखन) को संक्षेप में बताइए।
11. क्रिप्टोग्राफी (कूटलेखन) के संदर्भ से क्या समझते हैं?
12. क्रिप्टोग्राफी (कूटलेखन) की सुरक्षा सेवाओं को बताइए।
13. क्रिप्टोग्राफी (कूटलेखन) प्राथिमिकी क्या है?
14. क्रिप्टोसिस्टम (कूटतंत्र) की अवधारणा को स्पष्ट कीजिए।
15. क्रिप्टोसिस्टम (कूटतंत्र) की शक्ति से क्या समझते हैं?
16. क्रिप्टोसिस्टम (कूटतंत्र) का लक्ष्य क्या है?
17. क्रिप्टोसिस्टम (कूटतंत्र) के कौन–कौन से घटक हैं?
18. क्रिप्टोसिस्टम (कूटतंत्र) के प्रकार कौन–कौन से हैं?
19. सममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया) क्या है?
20. असममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया) से क्या समझते हैं?
21. सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) की चुनौती को स्पष्ट करें।
22. क्रिप्टोसिस्टम (कूटतंत्र) के लिए केर्कहोफ का सिद्वांत बताइए।
23. क्रिप्टोसिस्टम (कूटतंत्र) पर आक्रमण को समझाइए।
24. क्रिप्टोग्राफिक (कूटलेखीय) आक्रमण से क्या समझते हैं?
25. क्रिप्टोग्राफी (कूटलेखन) गुण और दोष लिखिए।
26. क्रिप्टोग्राफी (कूटलेखन) के अनुप्रयोग बताइए।
27. क्रिप्टोग्राफी (कूटलेखन) के भविष्य की अवधारणा को स्पष्ट कीजिए।

अध्याय – 2

प्राचीनकाल एन्क्रिप्शन (कूट प्रक्रिया)

प्राचीनकाल क्रिप्टोग्राफी (कूटलेखन), क्रिप्टोग्राफी (कूटलेखन) और उच्च स्तरीय गणित के पूर्व ज्ञान के बिना क्रिप्टोसिस्टम (कूटतंत्र) सीखने का सबसे अच्छा प्रारंभिक बिंदु है। यहां हम प्राचीनकाल क्रिप्टोसिस्टम (कूटतंत्र) की समीक्षा करेंगे। प्राचीनकाल क्रिप्टोसिस्टम (कूटतंत्र) से अर्थ यह है कि क्रिप्टोसिस्टम (कूटतंत्र) पेंसिल–और–पेपर आधारित हैं और बीसवीं शताब्दी के मध्य तक उपयोग किया जाता रहा है। इसमें शिफ्ट, एफिन, सरल प्रतिस्थापन, ट्रांसपोजिशन, हिल और विगेनियर सिफर (कूटलेख) शामिल हैं। प्राचीनकाल एन्क्रिप्शन को सममित कुंजी एन्क्रिप्शन भी कहते हैं जहां एन्क्रिप्शन और डिक्रिप्शन के लिए उपयोग की जाने वाली कुंजी समान है।

2.1 सीजर या विस्थापन सिफर (कूटलेख):

पहली शताब्दी B.C. में, जूलियस सीजर ने विस्थापन सिफर (कूटलेख) विकसित किया। विस्थापन कुंजी (shift key) के आधार पर, वर्णमाला में प्रत्येक अक्षर को नए स्थानांतरित अक्षर द्वारा प्रतिस्थापित किया जाता है। वह संदेश जिसे संगत नए अक्षर द्वारा प्रतिस्थापित करके एन्क्रिप्ट (कूटित) किया जाता है प्लेन–टेक्स्ट (साधारण–पाठ) कहा जाता है, और प्रतिस्थापन द्वारा उत्पादित नए संदेश को सिफर–टेक्स्ट (कूटलेख–पाठ) कहा जाता है। कुंजी अक्षरों की उस संख्या को वर्णित करता है जिसकी सहायता से प्लेन–टेक्स्ट (साधारण–पाठ) के अक्षर सिफर–टेक्स्ट (कूटलेख–पाठ) में प्रतिस्थापित होते हैं।

इसे मोनो–अल्फाबेटिक सिफर (कूटलेख–पाठ) भी कहते हैं जिसमें प्लेन–टेक्स्ट (साधारण–पाठ) के प्रत्येक अक्षर को सिफर–टेक्स्ट (कूटलेख–पाठ) बनाने के लिए दूसरे अक्षर द्वारा प्रतिस्थापित किया जाता है। यह प्रतिस्थापन सिफर (कूटलेख) योजना का एक सरल रूप है।

इस क्रिप्टोसिस्टम को आमतौर पर विस्थापन सिफर (कूटलेख) के रूप में जाना जाता है। अवधारणा प्रत्येक वर्णमाला को किसी अन्य वर्णमाला से प्रतिस्थापित करना है जिसे 0 और 25 के बीच कुछ निश्चित संख्या द्वारा स्थानांतरित किया जाता है।

इस प्रकार की योजना के लिए, प्रेषक और प्राप्तकर्ता दोनों वर्णमाला को स्थानांतरित करने के लिए गोपनीय विस्थापन संख्या पर सहमत होते हैं। यह संख्या जो 0 और 25 के मध्य होती है, एन्क्रिप्शन कुंजी बन जाती है। 'सीजर सिफर' नाम का प्रयोग कभी–कभी शिफ्ट सिफर का वर्णन करने के लिए भी किया जाता है।

निम्न उदाहरण देखें:

एन्क्रिप्शनः

दिया हैः विस्थापन कुंजी 5 है।

प्लेन–टेक्स्ट (साधारण–पाठ): I AM A STUDENT

प्लेन–टेक्स्ट (साधारण–पाठ) के प्रत्येक अक्षर को सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर में निम्न प्रकार परिवर्तित किया जाता हैः

I + Shift(5) = N
A + Shift(5) = F
M + Shift(5) = R
A + Shift(5) = F
S + Shift(5) = X
T + Shift(5) = Y
U + Shift(5) = Z
D + Shift(5) = I
E + Shift(5) = J
N + Shift(5) = S
T + Shift(5) = Y

अतः सिफर–टेक्स्ट (कूटलेख–पाठ) NFRFXYZIJSY होगा।

डिक्रिप्शनः

सिफर–टेक्स्ट (कूटलेख–पाठ) के प्रत्येक अक्षर को प्लेन–टेक्स्ट (साधारण–पाठ) अक्षर में निम्न प्रकार परिवर्तित किया जाता हैः

N – Shift(5) = I
F – Shift(5) = A
R – Shift(5) = M
F – Shift(5) = A
X – Shift(5) = S
Y – Shift(5) = T
Z – Shift(5) = U
I – Shift(5) = D
J – Shift(5) = E
S – Shift(5) = N
Y – Shift(5) = T

अतः प्लेन–टेक्स्ट (साधारण–पाठ) IAMASTUDENT होगा।

दोषः चूंकि वर्णमाला में 26 अक्षर हैं, प्रत्येक अक्षर को 25 स्थानों तक स्थानांतरित किया जा सकता है। सिफर–टेक्स्ट (कूटलेख–पाठ) को तोड़ने के लिए, हम सभी संभावित प्लेन–टेक्स्ट (साधारण–पाठ) को सूचीबद्ध कर सकते हैं और सबसे उचित संदेश चुन सकते हैं।

उदाहरण के लिए, यदि हमारे पास सिफर–टेक्स्ट (कूटलेख–पाठ) FRFXYZIJSY है, तो संभावित प्लेन–टेक्स्ट (साधारण–पाठ) हैंः

विस्थापन	**प्लेन–टेक्स्ट (साधारण–पाठ)**
1	MEQEWXYHIRX
2	LDPDVWXGHQW
3	KCOCUVWFGPV
4	JBNBTUVEFOU
5	IAMASTUDENT
6	HZLZRSTCDMS
7	GYKYQRSBCLR
8	FXJXPQRABKQ
9	EWIWOPQZAJP
10	DVHVNOPYZIO
11	CUGUMNOXYHN
12	BTFTLMNWXGM
13	ASESKLMVWFL
14	ZRDRJKLUVEK
15	YQCQIJKTUDJ
16	XPBPHIJSTCI
17	WOAOGHIRSBH
18	VNZNFGHQRAG
19	UMYMEFGPQZF
20	TLXLDEFOPYE
21	SKWKCDENOXD
22	RJVJBCDMNWC
23	QIUIABCLMVB
24	PHTHZABKLUA
25	OGSGYZAJKTZ

एकमात्र उचित संदेश का पता लगाने के द्वारा, हम यह ज्ञात कर सकते हैं कि विस्थापन कुंजी 5 है और प्लेन–टेक्स्ट (साधारण–पाठ) IAMASTUDENT है।

सुरक्षा मूल्यः सीजर सिफर (कूटलेख) एक सुरक्षित क्रिप्टोसिस्टम (कूटतंत्र) नहीं है क्योंकि प्रयास करने के लिए केवल 26 संभावित कुंजी हैं। एक आक्रमणकर्ता उपलब्ध सीमित कम्प्यूटिंग संसाधनों के साथ एक विस्तृत कुंजी की खोज कर सकता है।

2.2 सरल प्रतिस्थापन सिफर (कूटलेख):

एक मोनोअल्फाबेटिक या सरल प्रतिस्थापन सिफर (कूटलेख) वह है जिसमें सिफर–टेक्स्ट (कूटलेख–पाठ) वर्णमाला प्लेन–टेक्स्ट (साधारण–पाठ) वर्णमाला का पुनर्गठन है। प्रतिस्थापन सिफर (कूटलेख) 26! संभावित क्रमचयों को रखता है, जो वास्तव में बहुत असुरक्षित हैं और आसानी से अक्षरों की आवृत्ति का उपयोग कर हल किया जा सकता है। सरल प्रतिस्थापन उन संदेशों को समझने के लिए एक सही विधि है जिन्हें दृष्टि से समझ कर आसानी से डिक्रिप्ट (अकूटित) किया जा सकता है।

यह सीजर सिफर (कूटलेख) का उन्नत रूप है। कुछ संख्याओं द्वारा अक्षर को स्थानांतरित करने के स्थान पर, यह योजना वर्णमाला में अक्षरों के कुछ क्रमपरिवर्तन का उपयोग करती है। उदाहरण के लिए, A.B…..Y.Z और Z.Y……B.A वर्णमाला में सभी अक्षरों के दो स्पष्ट क्रमपरिवर्तन हैं। क्रमपरिवर्तन कुछ भी नहीं है लेकिन वर्णमाला का एक जुड़ा हुआ समूह है।

वर्णमाला में 26 अक्षरों के साथ, संभावित क्रमचय 26! हैं, जो 4×10^{26} के बराबर है। प्रेषक और प्राप्तकर्ता इनमें से किसी भी संभावित क्रमपरिवर्तन को सिफर–टेक्स्ट (कूटलेख–पाठ) वर्णमाला के रूप में चयन कर सकता है। यह क्रमपरिवर्तन योजना की गुप्त कुंजी है।

प्रेषक और प्राप्तकर्ता किसी कीवर्ड या वाक्यांश पर निर्णय लेते हैं। इस दशा में, माना वाक्यांश "the cows go moo in the field" का प्रयोग करते हैं। प्लेन–टेक्स्ट (साधारण–पाठ) और सिफर–टेक्स्ट (कूटलेख–पाठ) को मुख्य वाक्यांश के विशिष्ट अक्षरों से बनाई जाने वाली कुंजी के साथ रखा गया है।

प्लेन–टेक्स्ट (साधारण–पाठ)	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
सिफर–टेक्स्ट (कूटलेख–पाठ)	T	H	E	C	O	W	S	G	M	I	N	F	L	D	A	B	J	K	P	Q	R	U	V	X	Y	Z

यहाँ सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षरों के प्रथम भाग को मुख्य वाक्यांश (किसी भी दोहराए गए अक्षरों को छोड़कर) के माध्यम से प्रतिचित्रित किया गया है और दूसरा भाग A से Z के क्रम में वर्णमाला के शेष अक्षरों का उपयोग करके बनाया गया है।

एन्क्रिप्शनः प्रेषक संदेश MEET ME AT FIVE O'CLOCK को प्राप्तकर्ता की ओर भेजने के लिए संदेश को एन्क्रिप्ट (कूटित) करता है। इस संदेश को एन्क्रिप्ट (कूटित) करने के लिए, उपरोक्त तालिका से प्रत्येक प्लेन–टेक्स्ट (साधारण–पाठ) अक्षर को उसके संगत सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर के साथ प्रतिचित्रित किया जाता है। निम्न तालिका देखें:

प्लेन–टेक्स्ट	**सिफर–टेक्स्ट**
M	L
E	O
T	Q
A	T
F	W
I	M
V	U
O	A
C	E
L	F
K	N

अतः एन्क्रिप्टेड (कूटित) संदेश LOOQLOTQWMUOAEFAEN है।

डिक्रिप्शनः

चूंकि प्राप्तकर्ता कुंजी वाक्यांश जानता है, इसलिए वह उपरोक्त तालिका की सहायता से सिफर–टेक्स्ट (कूटलेख–पाठ) को प्लेन–टेक्स्ट (साधारण–पाठ) में आसानी से परिवर्तित कर सकता है।

दोषः

सरल प्रतिस्थापन सिफर (कूटलेख) के साथ बड़ी समस्या यह है कि अक्षरों की आवृत्तियों को बिल्कुल छिपाया नहीं गया है। यदि सिफर–टेक्स्ट (कूटलेख–पाठ) LOOQLOTQWMUOAEFAEN हो, तो व्याख्या करने वाला प्रत्येक अक्षर की आवृत्तियों को देख सकता है और उन्हें अंग्रेजी की आवृत्तियों तुलना कर सकता है। जैसा कि यहाँ O का प्रयोग अनुमानित संदेश में चार बार किया गया है, और L, Q, A और E सभी दो बार दिखाई देते हैं। अंग्रेजी आवृत्तियों के लिए शीर्ष नौ अक्षर E, T, A, O, N, I, S, R और H हैं। एक अनुमान के रूप में, व्याख्या करने वाला निम्नानुसार अक्षरों को लिख सकता हैः

प्लेन–टेक्स्ट (साधारण–पाठ)	सिफर–टेक्स्ट (कूटलेख–पाठ)
O	E
L	A
Q	T
A	O
E	N

एक त्वरित समझने वाला परीक्षण उत्तर AEETAE?T???EON?ON? हो सकता है। यदि व्याख्या करने वाला O = E से सहमत होता है और देखता है कि पहला वाक्यांश MEET ME AT के रूप में समझ सकता है, तब वह शेष संदेश को आसानी से समझ सकता है।

सुरक्षा मूल्यः

सरल प्रतिस्थापन सिफर (कूटलेख) सीजर सिफर (कूटलेख) का उन्नत रूप है। कुंजियों की संभावित संख्या बड़ी है (26!) और यहाँ तक कि आधुनिक कम्प्यूटिंग प्रणाली अभी तक शक्तिशाली नहीं हैं। अतः प्रणली को तोड़ने के लिए एक बलपूर्वक आक्रमण आसानी से किया जा सकता है। हालांकि, सरल प्रतिस्थापन सिफर (कूटलेख) एक साधारण अभिकल्पना रखता है और यह त्रुटियों को अभिकल्पित करने के लिए प्रवण है, स्पष्ट क्रमपरिवर्तन का चयन कर क्रिप्टोसिस्टम (कूटतंत्र) आसानी से खंडित किया जा सकता है।

2.3 मोनोअल्फाबेटिक और पॉलीअल्फाबेटिक सिफर (कूटलेख):

मोनोल्फाबेटिक सिफर (कूटलेख) एक प्रतिस्थापन सिफर (कूटलेख) है जिसमें एक दी गई कुंजी के लिए, प्रत्येक मूल वर्णमाला के लिए सिफर (कूटलेख) वर्णमाला एन्क्रिप्शन (कूट प्रक्रिया) प्रक्रिया में तय किया जाता है। उदाहरण के लिए, यदि A को D के रूप में एन्क्रिप्ट (कूटित) किया गया है, तो उस प्लेन–टेक्स्ट (साधारण–पाठ) में प्रकट होने वाली किसी भी संख्या के लिए, A सदैव D में एन्क्रिप्ट (कूटित) किया जाएगा।

इसके पूर्व चर्चा किए गए प्रतिस्थापन सिफर मोनोल्फाबेटिक ही हैं। ये सिफर (कूटलेख) क्रिप्टैनालिसिस (कूटविश्लेषण) के लिए अतिसंवेदनशील होते हैं।

पॉलीएल्फाबेटिक सिफर (कूटलेख) एक प्रतिस्थापन सिफर है जिसमें एन्क्रिप्शन (कूट प्रक्रिया) प्रक्रिया के दौरान पृथक–पृथक स्थानों पर मूल वर्णमाला के लिए सिफर (कूटलेख) वर्णमाला भिन्न हो सकता है। अगले दो सिफर (कूटलेख), प्लेफेयर और विगेनियर पॉलीएल्फाबेटिक सिफर (कूटलेख) हैं।

एक सिफर (कूटलेख) पॉलीएल्फाबेटिक होता है यदि वर्णमाला का एक दिया गया अक्षर सदैव एक ही सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर द्वारा एन्क्रिप्ट (कूटित) नहीं किया जाएगा, और इसके परिणामस्वरूप, प्लेन–टेक्स्ट (साधारण–पाठ) वर्णमाला के एक समूह के अनुरूप सिफर–टेक्स्ट (कूटलेख–पाठ) वर्णमाला के एक समूह द्वारा वर्णित नहीं किया जा सकता है।

पॉलीएल्फाबेटिक सिफर (कूटलेख) को जनित करने की सबसे आसान विधि विभिन्न मोनोएल्फाबेटिक सिफर (कूटलेख) को संयोजित करना है।

मोनोएल्फाबेटिक सिफर (कूटलेख) के साथ एक समस्या यह है कि अक्षर एक भाषा में कुछ आवृत्ति के साथ होते हैं। इस आवृत्ति को प्लेन–टेक्स्ट (साधारण–पाठ) अक्षरों और अनुमानित संदेश के सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षरों के लिए तैयार किया जा सकता है, और, कुछ विश्लेषण के बाद, सिफर अपेक्षाकृत आसानी से खंडित हो जाता है।

होमोमोनिक सिफर (कूटलेख) सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षरों की आवृत्तियों को समान करके स्थिति को परिवर्तित कर देता है। यह निम्नलिखित नियमों का उपयोग करता हैः

- अद्वितीय डिक्रिप्शन के लिए, विशिष्ट प्लेन–टेक्स्ट (साधारण–पाठ) अक्षरों से संबंधित समूह पृथक होना चाहिए।
- प्लेन–टेक्स्ट (साधारण–पाठ) को आबंटित सिफर–टेक्स्ट (कूटलेख–पाठ) प्रतीकों की संख्या उस अक्षर की आवृत्ति द्वारा निर्धारित की जाती है।

2.4 प्लेफेयर सिफर (कूटलेख):

इस विधि में, सरल प्रतिस्थापन सिफर (कूटलेख) की तुलना में एकल अक्षरों के स्थान पर अक्षर के युग्म एन्क्रिप्ट (कूटित) किए जाते हैं।

प्लेफेयर सिफर (कूटलेख) में, आरंभ में एक कुंजी तालिका बनाई जाती है। मुख्य तालिका वर्णमाला का 5 × 5 ग्रिड है जो प्लेन–टेक्स्ट (साधारण–पाठ) को एन्क्रिप्ट (कूटित) करने के लिए कुंजी के रूप में कार्य करता है। 25 अक्षरों में से प्रत्येक अद्वितीय होना चाहिए और वर्णमाला (आमतौर पर J) का एक अक्षर तालिका से छोड़ा जाता है क्योंकि हमें 26 के स्थान पर केवल 25 वर्णमाला की आवश्यकता होती है। यदि प्लेन–टेक्स्ट (साधारण–पाठ) में J होता है, तो इसे I से प्रतिस्थापित किया जाता है।

उदाहरण के लिए यदि एक विशेष कुंजी पर प्रेषक और प्राप्तकर्ता सहमत हैं, माना 'TUTORIALS'। तब कुंजी तालिका में, सबसे पहले बाएं से दाएं की ओर जाते हुए वाक्यांश TUTORIALS के अक्षरों (प्रतिलिपि अक्षरों को छोड़कर) को रखा जावेगा। शेष तालिका प्राकृतिक क्रम में वर्णमाला के शेष अक्षरों से भरेगी।

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

प्लेफेयर सिफर (कूटलेख) की प्रक्रियाः

सर्वप्रथम प्लेन–टेक्स्ट (साधारण–पाठ) संदेश से दो–दो अक्षरों के युग्म तैयार करें। यदि अक्षरों की एक विषम संख्या है, तो अंतिम अक्षर में Z जोड़ा जाता है। माना हम "HIDE MONEY" संदेश एन्क्रिप्ट (कूटित) करना चाहते हैं, तो इसे निम्न प्रकार लिखा जाएगाः

HI DE MO NE YZ

एन्क्रिप्शन (कूट प्रक्रिया) के नियम निम्न हैंः

1. यदि दोनों अक्षर एक ही स्तम्भ में हैं, तो प्रत्येक अक्षर के नीचे के अक्षर लें (यदि अक्षर सबसे नीचे है, तो शीर्ष पर वापस जाकर अक्षर का चयन करें)।

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

यहाँ H और I एक ही स्तम्भ में हैं, इसलिए उन्हें प्रतिस्थापित करने के लिए नीचे के अक्षर लें। इसप्रकार HI → QC में परिवर्तित हो जावेगा।

2. यदि दोनों अक्षर एक ही पंक्ति में हैं, तो प्रत्येक अक्षर के दाईं ओर के अक्षर का चयन करें (यदि अक्षर सबसे दाईं ओर हो, तो वापस बाईं ओर जावें)।

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

यहाँ D और E एक ही पंक्ति में हैं, इसलिए उन्हें प्रतिस्थापित करने के लिए दाईं ओर के अक्षर लें। इसप्रकार DE $\longrightarrow$ EF में परिवर्तित हो जावेगा।

3. यदि पूर्व दोनों नियमों में से कोई भी नियम लागू न हो, तो दोनों अक्षरों के साथ एक आयताकार घेरा बनाएं और अक्षरों के क्षैतिज विपरीत कोने पर के अक्षरों को लें।

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

यहाँ M और O न तो एक ही पंक्ति में हैं और न ही एक स्तम्भ में, अतः उन्हें प्रतिस्थापित करने के लिए विपरीत कोने पर के अक्षरों को लें। इसप्रकार MO $\longrightarrow$ NU में परिवर्तित हो जावेगा।

इन नियमों का उपयोग करके, 'TUTORIALS' कुंजी के साथ "HIDE MONEY" का एन्क्रिप्शन निम्न होगाः

QC EF NU MF ZV

प्लेफेयर सिफर (कूटलेख) को डिक्रिप्ट (अकूटित) करना, एक ही प्रक्रिया को विपरीत में करने जैसा आसान है। संदेश प्राप्तकर्ता समान कुंजी रखता है और वह समान कुंजी तालिका बना सकता है, और फिर उस कुंजी का उपयोग करके दिए गए किसी भी संदेश को डिक्रिप्ट (अकूटित) कर सकता है।

सुरक्षा मूल्यः

यह एक प्रतिस्थापन सिफर (कूटलेख) भी है और सरल प्रतिस्थापन सिफर (कूटलेख) की तुलना में खंडित करना मुश्किल है। प्रतिस्थापन सिफर (कूटलेख) की स्थिति में, प्लेफेयर सिफर (कूटलेख) पर क्रिप्टैनालिसिस (कूटविश्लेषण) भी संभव है, हालांकि यह 26 पृथक–पृथक संभावित अक्षरों के स्थान पर 625 संभावित अक्षरों (25×25 वर्णमाला) के लिए होगा।

प्लेफेयर सिफर (कूटलेख) मुख्य रूप से महत्वपूर्ण गोपनीय भेदों की रक्षा के लिए उपयोग किया जाता था, क्योंकि यह उपयोग करने में तेज है और इसके लिए कोई विशेष उपकरण की आवश्यकता नहीं है।

2.5 विगेनियर सिफर (कूटलेख):

विगेनियर सिफर (कूटलेख) एक पॉलीएल्फाबेटिक प्रतिस्थापन सिफर (कूटलेख) का एक उदाहरण है। एक पॉलीएल्फाबेटिक प्रतिस्थापन सिफर (कूटलेख) एक मोनोएल्फाबेटिक प्रतिस्थापन के समान होता है, अंतर मात्र यह है कि संदेश को समझते समय सिफर (कूटलेख) वर्णमाला समय–समय पर बदल जाता है। यह सिफर को अक्षर आवृत्तियों का उपयोग करके क्रिप्टैनालिसिस (कूटविश्लेषण) के लिए न्यून कर देता है।

इसे ब्लेज डी विगेनियर ने विकसित किया था जिसे 1585 में विगेनियर सिफर (कूटलेख) कहा जाने लगा। उन्होंने संदेशों को समझने के लिए विगेनियर स्क्वायर (Vigenère Square) के नाम से जानी जाने वाली एक तालिका का उपयोग किया। यहाँ हम विगेनियर सिफर (कूटलेख) की दो पृथक–पृथक विधियों यथा ऑटोकी (Autokey) विधि और कीवर्ड (Keyword) विधि पर चर्चा करेंगे।

1. ऑटोकी विधिः

एन्क्रिप्शनः

विगेनियर ऑटोकी विधि का उपयोग करके एक संदेश को समझने के लिए, प्रेषक और प्राप्तकर्ता को पहले प्राथमिक कुंजी पर सहमत होना चाहिए। प्राथमिक कुंजी एक एकल अक्षर है जिसे कुंजी बनाने के लिए संदेश के आरंभ में जोड़ा जाएगा। प्रेषक एक पंक्ति पर प्लेन–टेक्स्ट (साधारण–पाठ) लिखकर संदेश को एन्क्रिप्ट (कूटित) करेगा और इसके नीचे की रेखा पर कुंजी लिख देगा। प्रेषक विगेनियर वर्ग में एक पंक्ति और एक स्तम्भ का चयन करने के लिए प्लेन–टेक्स्ट (साधारण–पाठ) और कुंजी अक्षरों का उपयोग करेगा। चयनित पंक्ति वह पंक्ति है जिसमें प्लेन–टेक्स्ट (साधारण–पाठ) अक्षर प्रथम स्तम्भ में होता है और चयनित स्तम्भ वह स्तम्भ होता है जिसमें कुंजी अक्षर प्रथम पंक्ति में होता है। एक सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर वह अक्षर होगा जो विगेनियर स्क्वायर में चयनित पंक्ति और स्तम्भ के संगत स्थिति पर प्रकट होगा।

निम्नलिखित उदाहरण में, सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर खोजने के लिए, पहले विगेनियर स्क्वायर में उस पंक्ति का पता लगाएं जो प्लेन–टेक्स्ट (साधारण–पाठ) अक्षर T से मेल खाता है। तत्पश्चात् कुंजी अक्षर L के अनुरूप स्तम्भ का पता लगाएं। जिस अक्षर पर पंक्ति और स्तम्भ प्रतिच्छेद करते हैं वह सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर होगा, यहाँ सिफर टेक्स्ट (कूटलेख–पाठ) अक्षर E है। इसी क्रम को जारी रखते हुए अक्षरों के प्रत्येक युग्म के लिए सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर प्राप्त करें।

प्राथमिक कुंजी: L

प्लेन–टेक्स्ट	T O B E O R N O T T O B E
कुंजी	L T O B E O R N O T T O B
सिफर–टेक्स्ट	E H P F S F E B H M H P F

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

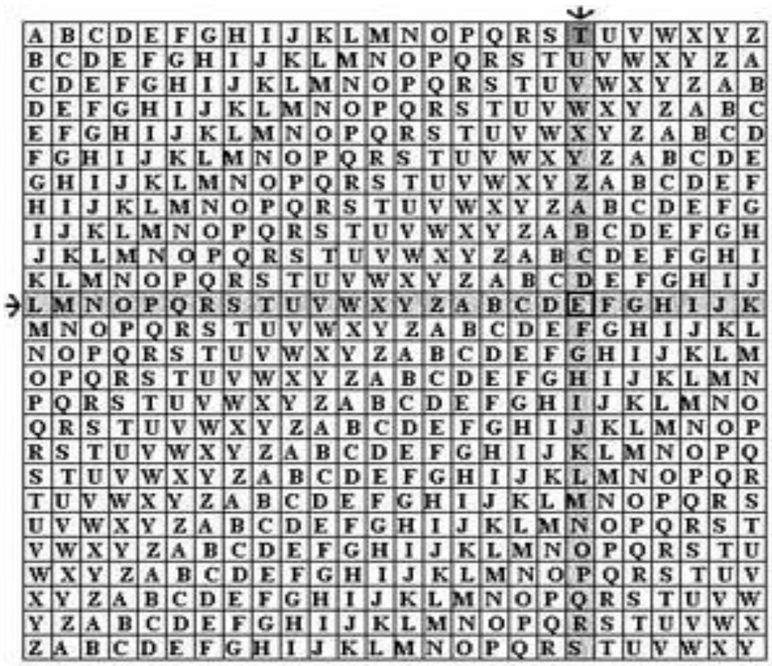
(चित्र क्र0 2.1; स्त्रोतः इंटरनेट से साभार)

डिक्रिप्शनः एक संदेश डिक्रिप्ट (अकूटित) करने के लिए, प्राथमिक कुंजी का उपयोग करके पंक्ति का चयन करते हैं। इसके उपरान्त, प्राप्तकर्ता चयनित पंक्ति में सिफर–टेक्स्ट (कूटलेख–पाठ) के प्रथम अक्षर को रेखांकित करता है। स्तम्भ के शीर्ष पर स्थित अक्षर जिसमें सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर होता है वह प्लेन–टेक्स्ट (साधारण–पाठ) का प्रथम अक्षर है। प्लेन–टेक्स्ट (साधारण–पाठ) के प्रथम अक्षर को कुंजी से जोड़ें और लगातार डिक्रिप्शन हेतु अगले सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षर के साथ इसका उपयोग करें।

उदाहरणः

संदेश: EHPFS FEBHM HPF
प्राथमिक कुंजी: L

कुंजी	E	H	P	F	S	F	E	B	H	M	H	P	F
सिफर–टेक्स्ट (कूटलेख–पाठ)	L	T	O	B	E	O	R	N	O	T	T	O	B
प्लेन–टेक्स्ट (साधारण–पाठ)	T	O	B	E	O	R	N	O	T	T	O	B	E



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

(चित्र क्र0 2.2; स्त्रोतः इंटरनेट से साभार)

सुरक्षा मूल्यः

विगेनियर ऑटोकी विधि बहुत सुरक्षित नहीं है। केवल 26 संभावित कुंजी (वर्णमाला के 26 अक्षर) हैं। कोड को एक संपूर्ण खोज के साथ आसानी से खंडित किया जा सकता है। कोई भी व्यक्ति जो ऑटोकी विधि का उपयोग करके एन्क्रिप्ट (कूटित) किए गए संदेश को पढ़ना चाहता है, उसे केवल वर्णमाला कुंजी के रूप में वर्णमाला के प्रत्येक अक्षर का उपयोग करने की आवश्यकता होती है जब तक कि वह एक समझ सकने योग्य संदेश नहीं बनाते। यह थोड़े समय में कम्प्यूटर के बिना भी किया जा सकता है। हालांकि, ऑटोकी विगेनियर सिफर (कूटलेख) के पीछे मूल विचार यह है कि इसका उपयोग कर एक सुरक्षित सिफर (कूटलेख) का उत्पादन किया जा सकता है।

2. कीवर्ड विधिः

एन्क्रिप्शनः

कीवर्ड विगेनियर सिफर (कूटलेख) ऑटोकी विधि के समान है, लेकिन इसमें एक एकल अक्षर प्राथमिक कुंजी का उपयोग करने के स्थान पर एक कीवर्ड का उपयोग किया जाता है। कीवर्ड किसी भी लंबाई की हो सकती है लेकिन एक से अधिक, जो संभावित कुंजी की असीमित संख्या प्रदान करती है। कुंजी बनाने के लिए, प्रेषक प्लेन–टेक्स्ट (साधारण–पाठ) के नीचे की पंक्ति पर बार–बार कीवर्ड लिखता है। तब विगेनियर स्क्वायर का उपयोग करके ऑटोकी विधि के समान प्रत्येक स्तम्भ में प्लेन–टेक्स्ट (साधारण–पाठ) और कुंजी का युग्म एन्क्रिप्ट (कूटित) किया जाएगा।

उदाहरणः

संदेशः "What fools these mortals be"

कीवर्डः Puck

प्लेन–टेक्स्ट (साधारण–पाठ)	W	H A T F	O O L S T	H E S E M	O R T A L	S B E
कुंजी	P	U C K P	U C K P U	C K P U C	K P U C K	P U C
सिफर–टेक्स्ट (कूटलेख–पाठ)	L	B C D U	I Q V H N	J O H Y O	Y G N C V	H V G

डिक्रिप्शनः

विगेनियर कीवर्ड विधि से एन्कोड किए गए संदेश को डिक्रिप्ट (अकूटित) करने के लिए, पहले बार–बार कुंजी लिखें। इसके नीचे सिफर–टेक्स्ट (कूटलेख–पाठ) लिखें। विगेनियर स्क्वायर का उपयोग करके कुंजी सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षरों के प्रत्येक युग्म को उसी तरह डीकोड करें, जैसे उन्हें ऑटोकी विधि के साथ डीकोड किया गया था।

उदाहरणः

संदेशः LBCDU IQVHN JOHYO YGNCV HVG

कीवर्डः Puck

कुंजी	P	U C K P	U C K P U	C K P U C	K P U C K	P U C
सिफर–टेक्स्ट (कूटलेख–पाठ)	L	B C D U	I Q V H N	J O H Y O	Y G N C V	H V G
प्लेन–टेक्स्ट (साधारण–पाठ)	W	H A T F	O O L S T	H E S E M	O R T A L	S B E

सुरक्षा मूल्यः

कीवर्ड विगेनियर सिफर (कूटलेख) ऑटोकी विधि से अधिक सुरक्षित है, लेकिन यह अभी भी कमजोर है। जितना लंबा कीवर्ड, उतना सुरक्षित सिफर (कूटलेख)। यदि कीवर्ड की लंबाई प्लेन–टेक्स्ट (साधारण–पाठ) के समान है, तो प्रत्येक संदेश के लिए एक नई कुंजी का उपयोग होने पर सिफर खंडित नहीं हो सकता है। माना हमें निम्न एन्क्रिप्टेड (कूटित) संदेश प्राप्त हुआ हैः

JTLOM FJRCS XM

यदि प्राप्तकर्ता कीवर्ड hfikeniaoitz का उपयोग करता है तो उसे निम्न संदेश प्राप्त होगाः

CODE IS BROKEN

यदि प्राप्तकर्ता कीवर्ड hfikenrnaygi का उपयोग करता है तो उसे निम्न संदेश प्राप्त होगाः

CODE IS SECURE

यहाँ तक कि यदि उचित समय में लंबाई 12 के सभी संभावित खोज शब्दों की गणना करना संभव था, तो सिफर–टेक्स्ट (कूटलेख–पाठ) लंबाई 12 के हर समझ सकने योग्य संदेश का उत्पादन करेगा। यह निर्धारित करने का कोई तरीका नहीं है कि प्रेषक किस संदेश को संवाद करने की अभिलाषा रखता है।

विगेनियर सिफर (कूटलेख) के प्रकारः

विगेनियर सिफर के दो विशेष प्रकार हैंः

1. कीवर्ड की लंबाई प्लेन–टेक्स्ट (साधारण–पाठ) संदेश के समान हो। इस स्थिति को वर्नम सिफर (कूटलेख) कहा जाता है। यह मूल विगेनियर सिफर (कूटलेख) से अधिक सुरक्षित है।
2. विगेनियर सिफर (कूटलेख) एक परिपूर्ण गुप्तता के साथ एक क्रिप्टोसिस्टम (कूटतंत्र) बन जाता है, जिसे वन–टाइम पैड कहा जाता है।

वन–टाइम पैडः

1. कीवर्ड की लंबाई प्लेन–टेक्स्ट (साधारण–पाठ) की लंबाई के समान है।
2. कीवर्ड वर्णमाला से यादृच्छिक रूप से जनित किया गया स्ट्रिंग हो।
3. कीवर्ड मात्र एक बार उपयोग किया जाता है।

सुरक्षा मूल्यः

हम विस्थापन सिफर (कूटलेख) की तुलना वन–टाइम पैड से करेंगे।

विस्थापन सिफर (कूटलेख) – खंडित करने में आसानः

विस्थापन सिफर (कूटलेख) की स्थिति में, पूरे संदेश में 1 और 25 के बीच बदलाव हो सकता है। यह एक बहुत छोटा आकार है, और इस पर आक्रमण करना बहुत आसान है। हालांकि, प्रत्येक कैरेक्टर (संप्रतीक) के साथ अब 1 और 26 के मध्य अपनी व्यक्तिगत विस्थापन होने के साथ, संभावित कुंजी संदेश के लिए तेजी से बढ़ती है।

वन–टाइम पैड – खंडित करना असंभवः

माना हम वन–टाइम पैड के साथ "point" को एन्क्रिप्ट (कूटित) करते हैं। यह एक 5 अक्षर का टेक्स्ट (पाठ) है। ब्रूट फोर्स द्वारा सिफर–टेक्स्ट (कूटलेख–पाठ) को खंडित करने के लिए, हमें कुजियों की सभी संभावनाओं का प्रयास करना होगा और $(26 \times 26 \times 26 \times 26 \times 26) = 265 = 11881376$ बार संगणना करने की आवश्यकता होगी। यह 5 अक्षरों वाले संदेश के लिए है। इस प्रकार, एक लंबे संदेश के लिए, गणना प्रत्येक अतिरिक्त वर्णमाला के साथ तेजी से बढ़ती है। यह ब्रूट फोर्स द्वारा सिफर–टेक्स्ट (कूटलेख–पाठ) को खंडित करने के लिए संगणित रूप से असंभव बनाता है।

विगेनियर सिफर (कूटलेख) क्रिप्टैनालिसिस (कूटविश्लेषण)ः

आरंभ में विगेनियर सिफर (कूटलेख) बहुत सुरक्षित लगता है, हालांकि कीवर्ड की लंबाई ज्ञात होने पर इसे आसानी से खंडित किया जा सकता है। यदि कीवर्ड की लंबाई n हो, तो हम सिफर–टेक्स्ट (कूटलेख–पाठ) को n उपसमूहों में खंडित कर सकते हैं और सिफर–टेक्स्ट (कूटलेख–पाठ) के पर्याप्त लम्बे होने पर आवृत्ति विश्लेषण का उपयोग करके सिफर (कूटलेख) पर आक्रमण कर सकते हैं। अब हम कीवर्ड की लंबाई निर्धारित करने के लिए दो विधियों फ्राइडमैन (Friedman) और कासिस्की (Kasisiki) परीक्षणों को देखेंगे।

1. फ्राइडमैन परीक्षणः

सिफर–टेक्स्ट (कूटलेख–पाठ) के नमूने के लिए संयोग की घटनाओं को ढूंढना यह इंगित कर सकता है कि एक संदेश को एन्क्रिप्ट (कूटित) करने के लिए पॉलीएल्फाबेटिक प्रतिस्थापन का उपयोग किया गया है या नहीं। संयोग की घटनाएं संभाव्यता है कि दो यादृच्छिक रूप से चयनित अक्षर समान हों। सामान्य अंग्रेजी में 0.065 के संयोग की घटनाएं होती हैं। यदि टेक्स्ट (पाठ) के नमूने में इस संख्या के करीब संयोग की घटनाएं होती हैं तो यह एक मोनोएल्फाबेटिक प्रतिस्थापन होने की संभावना है। यदि यह 0.0385 से बड़ा है और 0.065 से कम है तो टेक्स्ट को विगेनियर सिफर (कूटलेख) जैसे पॉलीएल्फाबेटिक सिफर (कूटलेख) का उपयोग करके सबसे अधिक संभावना माना जाता है। संयोग की घटनाओं को खोजने के लिए निम्न सूत्र हैः

$$I = \frac{1}{n(n-1)} \sum_{i=0}^{25} n_i \, (n_i - 1)$$

जहाँ $n_0, n_1, n_2, \ldots, n_{24}, n_{25}$ सिफर–टेक्स्ट (कूटलेख–पाठ) के नमूने में A, B, C,...,Y, Z की संबंधित संख्याएं हैं और $n = n_0 + n_1 + n_2 + \ldots + n_{24} + n_{25}$ (सिफरटेक्स्ट में अक्षरों की कुल संख्या)।

अनुमानित कीवर्ड लंबाई प्राप्त करने के लिए, निम्ने मान की गणना करेंः

$$k \approx \frac{0.0265n}{(0.065-I)+n(I-0.085)}$$

2. कासिस्की परीक्षणः

कासिस्की परीक्षण में कीवर्ड की लंबाई निर्धारित करने के लिए कीवर्ड के साथ अक्षर के समूहों के प्रासंगिक संरेखण का उपयोग किया जाता है। यह सिफर–टेक्स्ट (कूटलेख–पाठ) में अक्षरों के दोहराए गए समूहों का उत्पादन करता है। अक्षरों के इन दोहराए गए समूहों के आरंभ और वह संख्या जो उनकी दूरी के गुणत में हो के मध्य उपस्थित अक्षरों की संख्या की गणना कर हम कीवर्ड की लंबाई का अनुमान लगा सकते हैं।

उदाहरणः

प्लेन–टेक्स्ट (साधारण–पाठ)	THECHILDISTHEFATHEROFTHEMAN
कुंजी	POETRYPOETRYPOETRYPOETRY
सिफर–टेक्स्ट (कूटलेख–पाठ)	**IVE**VYGARMLMY**IVE**KFD**IVE**FRL

दोहराए गए अक्षरों का दूसरा IVE समूह प्रथम अक्षर के 12 अक्षर उपरान्त प्रकट होता है। इसीप्रकार IVE अक्षरों का तीसरा समूह 6 अक्षर उपरान्त दिखाई देता है। चूंकि इनमें से दोनों संख्या 6 के गुणक हैं, इससे पता चलता है कि कीवर्ड की लंबाई 6 है।

सुरक्षा मूल्यः

विगेनियर सिफर (कूटलेख) को सिफर–टेक्स्ट (कूटलेख–पाठ) पर क्रिप्टैनालिसिस की प्रभावशीलता को कम करने और क्रिप्टोसिस्टम (कूटतंत्र) को अधिक मजबूत बनाने के लिए मानक सीजर सिफर (कूटलेख) को परिवर्तित करके डिजाइन किया गया था। यह एक नियमित सीजर सिफर (कूटलेख) से काफी सुरक्षित है।

इतिहास में, नियमित रूप से संवेदनशील राजनीतिक और सैन्य सूचना की सुरक्षा के लिए इसका उपयोग किया जाता था। इसे क्रिप्टैनालिसिस (कूटविश्लेषण) के सामने आने वाली कठिनाई के कारण अखंडित सिफर (कूटलेख) के रूप में जाना जाता था।

2.6 ट्रान्सपोजीशन सिफर (कूटलेख):

यह एक अन्य प्रकार का सिफर (कूटलेख) है जहाँ सिफर–टेक्स्ट (कूटलेख–पाठ) बनाने के लिए प्लेन–टेक्स्ट (साधारण–पाठ) में वर्णमाला का क्रम पुनर्व्यवस्थित किया जाता है। वास्तविक प्लेन–टेक्स्ट (साधारण–पाठ) वर्णमाला प्रतिस्थापित नहीं होते हैं। इसका एक उदाहरण 'सरल स्तम्भ ट्रांसपोजिशन' (Simple columnar transposition) सिफर (कूटलेख) है, जहाँ प्लेन–टेक्स्ट (साधारण–पाठ) को एक निश्चित वर्णमाला चौड़ाई के साथ क्षैतिज रूप से लिखा जाता है। फिर नीचे दिखाए गए अनुसार सिफर–टेक्स्ट (कूटलेख–पाठ) लंबवत पढ़ा जाता है।

उदाहरण के लिए, प्लेन–टेक्स्ट (साधारण–पाठ) "golden statue is in eleventh cave" है और चयनित गुप्त यादृच्छिक कुंजी 5 है। हम तालिका में क्षैतिज रूप से इस टेक्स्ट (पाठ) को कुंजी मान के बराबर स्तम्भ की संख्या के साथ व्यवस्थित करते हैं। परिणामी टेक्स्ट (पाठ) नीचे दिखाया गया है।

g	o	l	d	e
n	s	t	a	t
u	e	i	s	i
n	e	l	e	v
e	n	t	h	c
a	v	e		

सिफर–टेक्स्ट (कूटलेख–पाठ) प्राप्त करने के लिए स्तम्भ को ऊपर से नीचे लंबवत पढ़कर प्राप्त किया जाता है। सिफर–टेक्स्ट (कूटलेख–पाठ) 'gnuneaoseenvltiltedasehetivc' है।

डिक्रिप्ट (अकूटित) करने के लिए, प्राप्तकर्ता समान तालिका तैयार करता है। स्तम्भ की संख्या कुंजी संख्या के बराबर है। पंक्तियों की संख्या कुल सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षरों की संख्या को कुंजी मान से विभाजित करके प्राप्त की जाती है और भागफल को आगामी पूर्णांक मान के लिए पूर्ण किया जाता है।

प्राप्तकर्ता तब प्राप्त सिफर–टेक्स्ट (कूटलेख–पाठ) को लंबवत नीचे की ओर बाएं से दाएं स्तम्भ में लिखता है। टेक्स्ट प्राप्त करने के लिए, वह क्षैतिज बाएं से दाएं और ऊपर से नीचे पंक्ति तक पढ़ता है।

विवरणः

एक ट्रांसपोजिशन सिफर (कूटलेख) अर्थ प्लेन–टेक्स्ट (साधारण–पाठ) के अक्षरों का क्रमपरिवर्तन (पुनर्गठन) करना है ताकि सिफर–टेक्स्ट (कूटलेख–पाठ) अच्छी तरह से एन्क्रिप्टेड दिखाई दे। ट्रांसपोजिशन सिफर (कूटलेख) बेहद सुरक्षित नहीं हैं क्योंकि वे प्लेन–टेक्स्ट (साधारण–पाठ) में अक्षरों को नहीं बदलते हैं या यहाँ तक कि आवृत्तियों को भी आच्छादित नहीं करते हैं, लेकिन इन्हें एन्क्रिप्शन के अधिक सुरक्षित तरीके बनाने के लिए बनाया जा सकता है। ट्रांसपोजिशन सिफर (कूटलेख) का एक उदाहरण रेल फेंस सिफर (कूटलेख) है।

उदाहरण के लिए रेल फेंस सिफर एक बहुत ही सरल स्तम्भ ट्रांसपोजिशन है जो एक स्ट्रिंग लेता है और अक्षरों को टेढा–तिरछे (zigzag) स्वरूप के माध्यम से दो समूहों में विभाजित करता है, जैसा कि नीचे दिखाया गया है।

एन्क्रिप्शनः

प्लेन–टेक्स्ट (साधारण–पाठ) = WHEN DRINKING WATER, REMEMBER ITS SOURCE
संपीड़ित प्लेन–टेक्स्ट (साधारण–पाठ) = WHENDRINKINGWATERREMEMBERITSSOURCE

zig: W E D I K N W T R E E B R T S U C
zag: H N R N I G A E R M M E I S O R E

zig = WEDIKNWTREEBRTSUC
zag = HNRNIGAERMMEISORE
सिफर–टेक्स्ट (कूटलेख–पाठ) = zig + zag
सिफर–टेक्स्ट (कूटलेख–पाठ) = WEDIKNWTREEBRTSUCHNRNIGAERMMEISORE

डिक्रिप्शनः

डिक्रिप्ट (अकूटित) करने के लिए सिफर–टेक्स्ट (कूटलेख–पाठ) को मध्य से विभाजित करें और दोनों सबस्ट्रिंग्स (उपरज्जु) से एकान्तर अक्षरों के साथ एक नई स्ट्रिंग बनाएं।

सबस्ट्रिंग_1 = WEDIKNWTREEBRTSUC
सबस्ट्रिंग_2 = HNRNIGAERMMEISORE
नवीन स्ट्रिंग = W + H + E + N + D + R + … + U + R + C + E

स्कैटल सिफर (कूटलेख):

चौथी शताब्दी B.C. में, स्पार्टन सरकार और सैन्य संदेशों को एन्क्रिप्ट (कूटित) करने के लिए स्कैटल नामक एक यंत्र का उपयोग किया था। इस यंत्र में लकड़ी के सिलेंडर में कागज की एक पट्टी उसके चारों ओर लपेटी गई थी। जब कागज हटा दिया जाता था, तो यह केवल मिश्रित अक्षरों की एक स्ट्रिंग थी, लेकिन यंत्र के चारों ओर लपेटते ही, संदेश स्पष्ट रूप से प्रकट हो जाता था। स्कैटल, रेल फेंस सिफर (कूटलेख) के समान ही कार्य करता है और संदेश को छुपाने में सहायता के लिए दी गई लंबाई की एक कुंजी का उपयोग करके उस पर विस्तार करता है।

एन्क्रिप्शनः

प्लेन–टेक्स्ट (साधारण–पाठ) = WHEN DRINKING WATER, REMEMBER ITS SOURCE
संपीड़ित प्लेन–टेक्स्ट (साधारण–पाठ) = WHENDRINKINGWATERREMEMBERITSSOURCE
संपीड़ित प्लेन–टेक्स्ट (साधारण–पाठ) की लंबाई = 34
चयनित कुंजी की लम्बाई = 4

कुंजी की लंबाई 4 से प्लेन–टेक्स्ट (साधारण–पाठ) की लंबाई 34 को विभाजित करने पर भागफल 8 तथा शेषफल 2 प्राप्त होता है। इसलिए हम स्कैटल की प्रत्येक पंक्ति की लंबाई 9 तक बढ़ाते हैं और z का दो बार उपयोग करते हुए संदेश को अक्षर z के साथ पैड करते हैं, क्योंकि अंतिम दो स्थान रिक्त हैं।

W	H	E	N	D	R	I	N	K
I	N	G	W	A	T	E	R	R
E	M	E	M	B	E	R	I	T
S	S	O	U	R	C	E	Z	Z

प्रत्येक स्तम्भ से अक्षरों को लेकर बाएं से दाएं चलते हुए हमें निम्न सिफर–टेक्स्ट (कूटलेख–पाठ) मिलता हैः

WIESHNMSEGEONWMUDABRRTECIERENRIZKRTZ

डिक्रिप्शनः

डिक्रिप्ट (अकूटित) करने के लिए, यह जानते हुए कि कुंजी का आकार 4 है, इसलिए हम पहले चार अक्षरों को ऊपर से नीचे तक लिखते हैं, फिर आसन्न स्तम्भ में आगामी चार अक्षरों को इसी प्रकार से लिखते हैं। प्रत्येक पंक्ति से अक्षरों को पढ़ना और अंतिम पैडेड अक्षरों को छोड़ने पर हमें प्लेन–टेक्स्ट (साधारण–पाठ) प्राप्त होता है।

दोषः

छोटे संदेशों की स्थिति में, सिफर–टेक्स्ट (कूटलेख–पाठ) को आसानी से पृथक–पृथक महत्वपूर्ण मानों के साथ डिक्रिप्ट (अकूटित) करने के लिए तैयार किया जाता है। सिफरटेक्स्ट (कूटलेख–पाठ) जिसकी लंबाई 36 हो 3 से विभाजित होता है, इसलिए हम पहले कुंजी 3 के साथ परीक्षण करते हैं, जिसके परिणामस्वरूप –

WSMGNUBTIEIR
IHSEWDREENZT
ENEOMARCRRKZ

इसे पंक्ति–दर–पंक्ति पढ़ते समय स्पष्ट रूप से कोई सार्थक संदेश नहीं प्राप्त होता है, अतः हम यह समझ सकते हैं कि कुंजी 3 नहीं है।

अब हम कुंजी 6 के साथ परीक्षण करते हैं, जो 36 को विभाजित करता है, हमें प्राप्त होता है ...

WMNBII
ISWREZ
EEMRRK
SGUTER
HEDENT
NOACRZ

जो फिर से सही टेक्स्ट नहीं है। वास्तव में, हमें यहाँ पूरे उत्तर का भी प्रबंध नहीं करना पड़ेगा, क्योंकि दूसरे स्तम्भ में रखने के उपरान्त, हमारा पहला शब्द WM के साथ आरंभ हुआ था, और कोई भी अंग्रेजी भाषा शब्द इस प्रकार से आरंभ नहीं होता है। इसलिए कुंजी 6 कार्य नहीं करेगी।

अतः लंबाई 4 की कुंजी का उपयोग करने पर सही उत्तर प्राप्त होगाः

WHENDRINK
INGWATERR
EMEMBERIT
SSOURCEZZ

अतः हमें निम्न प्लेन–टेक्स्ट (साधारण–पाठ) प्राप्त होगा, जो सही उत्तर हैः

WHENDRINKINGWATERREMEMBERITSSOURCEZZ

पंक्ति ट्रांसपोजिशन सिफर (कूटलेख):

- सामान्यतः कई स्तम्भ में संदेश लिखें और फिर इन स्तम्भ से पढ़ने के लिए कुछ नियमों का उपयोग करें।
- कुंजी संख्या की एक श्रृंखला हो सकती है। सिफर को पढ़ें या प्लेन–टेक्स्ट (साधारण–पाठ) में लिखें।

उदाहरणः

प्लेन–टेक्स्ट (साधारण–पाठ): THESIMPLESTPOSSIBLETRANSPOSITIONSXX

कुंजी (R):	2 5 4 1 3	
कुंजी (W):		4 1 5 3 2
	T H E S I	S T I E H
	M P L E S	E M S L P
	T P O S S	S T S O P
	I B L E T	E I T L B
	R A N S P	S R P N A
	O S I T I	T O I I S
	O N S X X	X O X S N

सिफर–टेक्स्ट (कूटलेख–पाठ): STIEH EMSLP STSOP EITLB SRPNA TOIIS XOXSN

पंक्ति ट्रांसपोजिशन सिफर (कूटलेख) के क्रिप्टैनालिसिस (कूटविश्लेषण):

- आवृत्ति गणना एक सामान्य भाषा रूपरेखा दिखाएगी।
- इसलिए अक्षरों को पुनः व्यवस्थित किया गया है।
- मूल विचार अवधि का अनुमान लगाना है, फिर अवधि में सभी संभावित क्रमिकताओं को देखें, और सार्व प्रारूप की खोज करें।
- सार्व युग्म और त्रिक तथा अन्य सुविधाओं की सूचियों का उपयोग करें।

ब्लॉक ट्रांसपोजिशन सिफर (कूटलेख):

सिफर (कूटलेख) का एक और प्रकार ब्लॉक ट्रांसपोजिशन सिफर (कूटलेख) है, जहाँ संदेश पंक्तियों में लिखा गया है, लेकिन वापसी की आसानी के लिए कुंजी (क्रिप्टो में B कमांड का उपयोग करें) द्वारा दिए गए क्रम में स्तम्भ को पढ़ा जाता है।

कुंजी (R):	s o r c e r y	s o r c e r y
कुंजी (R):	6 3 4 1 2 5 7	6 3 4 1 2 5 7
	l a s e r b e	l a s e r b e
	a m s c a n b	a m s c a n b
	e m o d u l a	e m o d u l a
	t e d t o c a	t e d t o c a
	r r y m o r e	r r y m o r e
	i n t e l l i	i n t e l l i
	g e n c e t h	g e n c e t h
	a n r a d i o	a n r a d i o
	w a v e s	w a v e s q r

यह निम्न सिफर–टेक्स्ट (कूटलेख–पाठ) देगा (स्तम्भ 4, 5, 2, 3, 6, 1, 7 को पढ़कर)

ecdtm ecaer auool edsam merne nasso dytnr vbnlc rltiq laetr igawe baaei hor

डिक्रिप्शन में निम्न शामिल हैं:

- गणना करें कि वहाँ कितनी पंक्तियां हैं (कुंजी की लंबाई से संदेश की लंबाई को विभाजित करके)।
- फिर कुंजी द्वारा दिए गए क्रम में कॉलम से संदेश लिखें।

2.7 एफिन सिफर (कूटलेख):

चूंकि एक शिफ्ट सिफर–टेक्स्ट (कूटलेख–पाठ) के लिए केवल 25 पृथक–पृथक परिवर्तनों का उत्पादन कर सकता है, इसलिए यह बहुत ही सुरक्षित एन्क्रिप्शन विधि नहीं है। एफिन सिफर (कूटलेख), विस्थापन सिफर (कूटलेख) का एक सामान्यीकरण है जो थोड़ा और अधिक सुरक्षा प्रदान करता है। निम्न फलन का उपयोग करके प्रत्येक अक्षर के लिए एफिन सिफर (कूटलेख) गुणा और योग लागू करता है।

$$y = (ax + b) \text{ MOD } m$$

जहाँ x प्लेन–टेक्स्ट (साधारण–पाठ) में अक्षर का संख्यात्मक मान है, m प्लेन–टेक्स्ट (साधारण–पाठ) वर्णमाला में अक्षरों की संख्या है, a और b गुप्त संख्या हैं, और y परिवर्तन का परिणाम है। y को सूत्र x = inverse(a) (y – b) MOD m का उपयोग कर x पर वापस डिक्रिप्ट (अकूटित) किया जा सकता है, inverse(a) एक मान इस प्रकार है कि यदि यह a MODm के साथ गुणा हो तो परिणाम 1 होगा, अर्थात् (a * inverse(a)) MOD m = 1।

चूंकि गणना में मॉड्यूलो 26 अंकगणित शामिल है, अतः यदि गुणक 26 के साथ एक सार्व विभाजक रखता है, तो कई अक्षरों को अद्वितीय रूप से डीकोड नहीं किया जा सकता है। इसलिए, a और m का महत्तम सार्व विभाजक 1 होना चाहिए।

उदाहरणः

एन्क्रिप्शनः

माना संदेश को फलन y = (11x + 4) MOD 26 द्वारा एन्क्रिप्ट (कूटित) किया गया है। प्लेन–टेक्स्ट (साधारण–पाठ) MONEY को एन्क्रिप्ट (कूटित) करने के लिए, हम सर्व प्रथम प्लेन–टेक्स्ट (साधारण–पाठ) के प्रत्येक अक्षर को निम्नलिखित सूची के अनुसार 0 और 25 के मध्य के संख्यात्मक मान में परिवर्तित करते हैं।

A – 0
B – 1
C – 2
D – 3
.
Z - 25

इस प्रकार, प्लेन–टेक्स्ट (साधारण–पाठ) MONEY से संबंधित संख्यात्मक मान 12, 14, 13, 4, और 24 हैं। प्रत्येक संख्यात्मक मान के लिए दिए गए फलन को लागू करने पर हमें प्राप्त होता हैः

M: y = (11*12 + 4) MOD 26 = 6
O: y = (11*14 + 4) MOD 26 = 2
N: y = (11*13 + 4) MOD 26 = 17
E: y = (11*4 + 4) MOD 26 = 22
Y: y = (11*24 + 4) MOD 26 = 8

अतः संगत सिफर–टेक्स्ट (कूटलेख–पाठ) हैः

GCRWI

डिक्रिप्शनः

डिक्रिप्शन करने के लिए हम फलन y को निम्न प्रकार रूपान्तरित करते हैंः

x = inverse (a) (y – b) MOD m

तब हमें प्राप्त होता हैः

x = inverse(11) (y – 4) MOD 26

यहाँ inverse(11) MOD 26 = 19 है, तब डिक्रिप्शन फलन x = 19 (y – 4) MOD 26 होगा।

अब हम डिक्रिप्शन फलन को लागू करके सिफर–टेक्स्ट GCRWI को डिक्रिप्ट (अकूटित) करते हैं। हमें प्राप्त होता हैः

G: x = 19*(6-4) MOD 26 = 12
C: x = 19*(2-4) MOD 26 = 14
R: x = 19*(17-4) MOD 26 = 13
W: x = 19*(22-4) MOD 26 = 4
I: x = 19*(8-4) MOD 26 = 24

अतः संगत प्लेन–टेक्स्ट (साधारण–पाठ) हैः

MONEY

विश्लेषणः

चूंकि हम जानते हैं कि प्लेन–टेक्स्ट (साधारण–पाठ) में प्रत्येक अक्षर फलन $y = (ax + b)$ MOD m द्वारा एन्क्रिप्ट (कूटित) होता है, अतः हम x और y के दो उदाहरणों के साथ दो रैखिक समीकरणों को हल करके एफिन सिफर (कूटलेख) को खंडित कर सकते हैं। एक बार जब हम a और b के मान प्राप्त करते हैं, तो हम पूरे सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट कर सकते हैं।

2.8 निहिलिस्ट सिफर (कूटलेख):

एक जटिल ट्रांस्पोजीशन सिफर (कूटलेख) जो पंक्ति और स्तम्भ ट्रांस्पोजीशन दोनों का उपयोग करता है, निहिलिस्ट सिफर (कूटलेख) कहलाता है।

- कुंजी द्वारा नियंत्रित क्रम में पंक्तियों में संदेश लिखें (जैसा कि पंक्ति सिफर के लिए)।
- फिर पंक्तियों द्वारा पढ़ें, लेकिन कुंजी द्वारा नियंत्रित क्रम में, इस बार बगल में लिखें।
- कुंजी लंबाई के वर्ग के आकार की अवधि का उपयोग करें।

प्लेन–टेक्स्ट (साधारण–पाठ): NOWISTHETIMEFORALLGOODMEN

कुंजी (W):	L E M O N
	2 1 3 5 4
L 2	O N W S I
E 1	H T E I T
M 3	E M F R O
O 5	L A L O G
N 4	D O M N E

निहिलिस्ट सिफर (कूटलेख): HTEIT ONWSI EMFRO DOMNE LALOG

2.9 प्रोडक्ट सिफर (कूटलेख):

हम देख सकते हैं कि केवल प्रतिस्थापन या केवल ट्रांस्पोजीशन के आधार पर जनित सामान्य सिफर (कूटलेख) सुरक्षित नहीं हैं। दो प्रतिस्थापन वास्तव में केवल एक और जटिल प्रतिस्थापन है। दो ट्रांस्पोजीशन वास्तव में केवल एक और जटिल ट्रांस्पोजीशन है। लेकिन एक प्रतिस्थापन के बाद एक ट्रांस्पोजीशन एक नया बहुत कठिन सिफर बनाता है।

प्रोडक्ट सिफर (कूटलेख) में प्रतिस्थापन–ट्रांस्पोजीशन संयोजन एक साथ संयोजित होते हैं। सामान्यतः पेपर–पेंसिल द्वारा डिक्रिप्ट करना बहुत कठिन होता है। हालांकि एक प्रसिद्ध प्रोडक्ट सिफर (कूटलेख) ADFGVX का उपयोग प्रथम विश्व युद्ध में किया गया था।

ADFGVX प्रोडक्ट सिफर (कूटलेख):

- नाम के अनुरूप केवल ADFGVX अक्षरों का उपयोग किया जाता है।
- चुना गया बहुत अलग मोर्स कोड है।
- प्रत्येक प्लेन–टेक्स्ट (साधारण–पाठ) अक्षर को एक अक्षर युग्म (पंक्ति–स्तम्भ सूची) पर प्रतिचित्रित करने के लिए एक निश्चित प्रतिस्थापन तालिका का उपयोग करता है।
- फिर एक कुंजी ब्लॉक ट्रांस्पोजीशन का उपयोग करता है।

प्रतिस्थापन तालिकाः

\\	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

प्लेन–टेक्स्ट (साधारण–पाठ): PRODUCTCIPHERS
मध्यवर्ती–टेक्स्ट:

FG AG VD VF XA DG XV
DG XF FG VG GA AG XG

कुंजीयुक्त ब्लॉक कॉलम ट्रांसपोजिशन आव्यूहः

D	E	U	T	S	C	H	Key
2	3	7	6	5	1	4	Sorted Order
F	G	A	G	V	D	V	
F	X	A	D	G	X	V	
D	G	X	F	F	G	V	
G	G	A	A	G	X	G	

सिफर–टेक्स्ट (कूटलेख–पाठ): DXGX FFDG GXGG VVVG VGFG CDFA AAXA

2.10 हिल सिफर (कूटलेख):

हिल सिफर (कूटलेख) ब्लॉक सिफर (कूटलेख) का एक उदाहरण है। एक ब्लॉक सिफर (कूटलेख) वह सिफर (कूटलेख) होता है जिसमें अक्षरों के समूह को समान लंबाई वाले ब्लॉक में एक साथ एन्क्रिप्ट किया जाता है। हिल सिफर (कूटलेख) लेस्टर हिल द्वारा विकसित किया गया था। निम्न उदाहरण देखें:

एन्क्रिप्शनः

हिल सिफर (कूटलेख) का उपयोग करके एक संदेश को एन्क्रिप्ट (कूटित) करने के लिए, प्रेषक और प्राप्तकर्ता को पहले $n \times n$ आकार के एक कुंजी आव्यूह A पर सहमत होना चाहिए। A को mod 26 के लिए व्युत्क्रमणीय होना चाहिए। तब प्लेन–टेक्स्ट आकार n के ब्लॉक में एन्क्रिप्ट (कूटित) होगा। निम्नलिखित उदाहरण में A एक 2×2 आव्यूह है और संदेश 2 अक्षरों के ब्लॉक में एन्क्रिप्ट (कूटित) होगा।

कुंजी आव्यूह: $A = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix}$

संदेश: MISSISSIPPI

आव्यूह $\begin{bmatrix} 12 \\ 8 \end{bmatrix}$ के संगत प्रथम ब्लॉक MI है। तब प्रेषक गणना करता है:

$$A \begin{bmatrix} 12 \\ 8 \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \end{bmatrix} \pmod{26}$$

सिफर–टेक्स्ट (कूटलेख–पाठ) के पहले दो अक्षर 2, 8 के अनुरूप हैं और इसलिए CI हैं। पूरे प्लेन–टेक्स्ट (साधारण–पाठ) के लिए इस प्रक्रिया की पुनरावृत्ति की जावेगी। यदि 2 के ब्लॉक बनाने के लिए पर्याप्त अक्षर नहीं हैं, तो कुछ अक्षर के साथ संदेश को पैड करें, माना Z।

अतः संदेश MI SS IS SI PP IK निम्न में एन्क्रिप्ट हो जावेगा:

CI KK GE UW ER OY

स्मरण रहे कि दोहराए गए संयुक्ताक्षर IS, SS और प्लेन–टेक्स्ट (साधारण–पाठ) में दोहराए गए अक्षर S और P को हिल सिफर (कूटलेख) का उपयोग करके छिपाया जाता है।

डिक्रिप्शनः

एक संदेश को डिक्रिप्ट (अकूटित) करने के लिए, पहले कुंजी A के व्युत्क्रम की गणना करें।

$$A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (\text{mod} 26)$$

फिर प्लेन–टेक्स्ट (साधारण–पाठ) को पुनः प्राप्त करने के लिए सिफर–टेक्स्ट (कूटलेख–पाठ) अक्षरों (मॉड 26) के प्रत्येक युग्म द्वारा कुंजी के व्युत्क्रम को गुणा करें।

कुंजी आव्यूह: $A = \begin{bmatrix} 3 & 17 \\ 8 & 25 \end{bmatrix}$

एन्क्रिप्ट (कूटित) संदेश: CIKKGEUWEROY

संदेश को डिक्रिप्ट (अकूटित) करने के लिए प्राप्तकर्ता गणना करेगाः

$A^{-1}\begin{bmatrix}2\\8\end{bmatrix}=\begin{bmatrix}12\\8\end{bmatrix} \pmod{26}$

पहले दो अक्षर 12, 8 हैं जो M और I के अनुरूप हैं। प्राप्तकर्ता मूल संदेश MISSISSIPPIK को पुनर्प्राप्त करने के लिए सिफर–टेक्स्ट (कूटलेख–पाठ) में अक्षरों के प्रत्येक युग्म के लिए इस चरण को दोहराएगा।

विभिन्न ब्लॉक आकार के साथ एक हिल सिफर (कूटलेख) का उपयोग करने के लिए आव्यूह A में पंक्तियों और स्तंभों की संख्या ब्लॉक आकार के बराबर होनी चाहिए। उदाहरण के लिए यदि ब्लॉक आकार 4 है तो A का आकार 4 × 4 का आव्यूह होना चाहिए।

2.11 विभिन्न विधियों के लिए कम्प्यूटर प्रोग्रामः

1. सीजर विधि के लिए C प्रोग्रामः

Encryption

```
#include<stdio.h>
int main()
{
	char message[100], ch;
	int i, key;
	printf("Enter a message to encrypt: ");
	gets(message);
	printf("Enter key: ");
	scanf("%d", &key);
	for(i = 0; message[i] != '\0'; ++i){
		ch = message[i];
		if(ch >= 'a' && ch <= 'z'){
			ch = ch + key;

			if(ch > 'z'){
				ch = ch - 'z' + 'a' - 1;
			}
			message[i] = ch;
		}
		else if(ch >= 'A' && ch <= 'Z'){
			ch = ch + key;
			if(ch > 'Z')
			{
				ch = ch - 'Z' + 'A' - 1;
			}
			message[i] = ch;
		}
	}
	printf("Encrypted message: %s", message);
	return 0;
}
```

Output

```
Enter a message to encrypt: axzd
Enter key: 4
Encrypted message: ebdh
```

Decryption

```
#include<stdio.h>
int main()
{
	char message[100], ch;
	int i, key;
	printf("Enter a message to decrypt: ");
	gets(message);
	printf("Enter key: ");
	scanf("%d", &key);
	for(i = 0; message[i] != '\0'; ++i){
		ch = message[i];
		if(ch >= 'a' && ch <= 'z'){
			ch = ch - key;
			if(ch < 'a'){
				ch = ch + 'z' - 'a' + 1;
			}
			message[i] = ch;
		}
		else if(ch >= 'A' && ch <= 'Z'){
			ch = ch - key;
			if(ch < 'A'){
				ch = ch + 'Z' - 'A' + 1;
			}
			message[i] = ch;
		}
	}
	printf("Decrypted message: %s", message);
	return 0;
}
```

Output

```
Enter a message to decrypt: ebdh
Enter key: 4
Decrypted message: axzd
```

2. प्रतिस्थापन विधि के लिए C प्रोग्रामः

```
#include<stdio.h>
int main()
{
  char *message,*emessage,*dmessage;
  int i,j=0,k,key,temp;
```

```
  clrscr();
  printf("\nEnter the key\n");
  scanf("%d",&key);
  key=key%26;
  printf("\nEnter message\n");
  fflush(stdin);
  gets(message);
  for(i=0;message[i]!=NULL;i++)
  message[i]=tolower(message[i]);
  for(i=0;message[i]!=NULL;i++)
  {
  //printf("%c ",message[i]);
    if(message[i]==' ')
    emessage[j++]=message[i];
    else
        {
       if(message[i]>=48 && message[i]<=57)
       {
        temp=message[i]+key;
         if(temp>57)
         emessage[j++]=48+(temp-58);
         else
         emessage[j++]=temp;
       }
       else
           {
        if(message[i]>=97 && message[i]<=123)
          {
           temp=message[i]+key;
           if(temp>122)
             emessage[j++]=97+(temp-123);
           else
             emessage[j++]=temp;
           }
         else
              emessage[j++]=message[i];
        }
              // printf("%c ",emessage[j]);
    }
  }
  emessage[j]='\0';
  printf("\n\n\nEncrypted message is\n\n");
  for(i=0;emessage[i]!=NULL;i++)
  printf("%c",emessage[i]);
// printf("\n end");
for(i=0,j=0;emessage[i]!=NULL;i++)
```

```
  {
    if(emessage[i]==' ')
   dmessage[j++]=emessage[i];
    else
{

   if(emessage[i]>=48 && emessage[i]<=57)
      {
       temp=emessage[i]-key;
       if(temp<48)
       dmessage[j++]=58-(48-temp);
       else
       dmessage[j++]=temp;
      }
    else
       {
      if(emessage[i]>=97 && emessage[i]<=123)
        {
         temp=emessage[i]-key;
         if(temp<97)
         dmessage[j++]=123-(97-temp);
         else
         dmessage[j++]=temp;
        }
       else
        dmessage[j++]=emessage[i];
       }
   }
  }
  dmessage[j]='\0';
 printf("\n\n\nRetrieved message is\n\n");
 for(i=0;dmessage[i]!=NULL;i++)
 printf("%c",dmessage[i]);
 getch();
 return(0);
}
```

Output:

```
Enter the Key
3
Enter Message
Hello
Encrypted Message is
khoor
Retrieved message is
Hello
```

3. प्लेफेयर विधि के लिए **C** प्रोग्रामः

Encryption

```
#include<stdio.h>
int main(){
 char arr[5][5]={"MONAR","CHYBD","EFGIK","LPQST","UVWXZ"};
 char pt[10];
 int i, j, r1=0, r2=0, c1=0, c2=0;
 printf("Playfair Keymatrix\n=================\n");
 for(i=0; i<5; i++)
 {
  for(j=0; j<5; j++)
  printf("%c ", arr[i][j]);
  printf("\n");
 }
 printf("Enter your plain text:");
 scanf("%s",pt);
 printf("Your plain text = %s", pt);
 for(i=0; i<5; i++)
 {
  for(j=0; j<5; j++)
  {
    if(arr[i][j] == pt[0])
    {
     r1=i; c1=j;
    }
    if(arr[i][j] == pt[1])
    {
     r2=i; c2=j;
    }
  }
 }
 if(r1==r2) //when both characters in same row
 {
  if(c2==4) //for char in last column
    printf("Ciphertext = %c%c \n", arr[r1][c1+1], arr[r2][0]);
  else
    printf("Ciphertext = %c%c \n", arr[r1][c1+1], arr[r2][c2+1]);
 }
 if(c1==c2)//when both characters in same column
 {
  if(r2==4) //for char in last row
    printf("Ciphertext = %c%c \n", arr[r1+1][c1], arr[0][c2]);
  else
    printf("Ciphertext = %c%c \n", arr[r1+1][c1], arr[r2+1][c2]);
 }
 //when characters are not in a same row and column
```

```
 if(r1 != r2 && c1 != c2)
 {
   printf("\nCiphertext = %c%c \n", arr[r1][c2], arr[r2][c1]);
 }
 return 0;
}
```

Output:

```
Playfair Keymatrix
=================
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
Enter your plain text:IN
 Your plain text = IN
Ciphertext = GA
```

Decryption

```
#include<stdio.h>
int main()
{
 char arr[5][5]={"MONAR","CHYBD","EFGIK","LPQST","UVWXZ"};
 char ct[10];
 int i, j, r1=0, r2=0, c1=0, c2=0;
 printf("Plaifair Keymatrix\n=================\n");
 for(i=0; i<5; i++)
 {
  for(j=0; j<5; j++)
   printf("%c ", arr[i][j]);
  printf("\n");
 }
 printf("Enter your cipher text:");
 scanf("%s",ct);
 printf("Your cipher text is %s\n", ct);
 for(i=0; i<5; i++)
 {
  for(j=0; j<5; j++)
  {
   if(arr[i][j] == ct[0])
   {
    r1=i; c1=j;
   }
   if(arr[i][j] == ct[1])
   {
```

```
   r2=i; c2=j;
  }
 }
}
if(r1==r2) //Rule2-when both characters in same row
{
 if(c2==0) //for char in last column
  printf("Plaintext = %c%c \n", arr[r1][c1-1], arr[r2][4]);
 else
  printf("Plaintext = %c%c \n", arr[r1][c1-1], arr[r2][c2-1]);
}
if(c1==c2)//Rule3- when both characters in same column
{
 if(r2==0) //for char in last row
  printf("Plaintext = %c%c \n", arr[r1-1][c1], arr[4][c2]);
 else
  printf("Plaintext = %c%c \n", arr[r1-1][c1], arr[r2-1][c2]);
}
//Rule4 when characters are not in a same row and column
if(r1 != r2 && c1 != c2)
{
 printf("Plaintext = %c%c \n", arr[r1][c2], arr[r2][c1]);
}
return 0;
}
```

Output:

```
Plaifair Keymatrix
=================
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
Enter your cipher text:NA
Your cipher text is NA
Plaintext = ON
```

4. विगेनियर विधि के लिए C प्रोग्रामः

```
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
int main()
{
    int count, j;
    char message[50];
    char key[20];
```

```
    printf("\nEnter Message To Encode:\t");
    fflush(stdin);
    scanf("%[^\n]s", message);
    printf("\nEnter Key:\t");
    fflush(stdin);
    scanf("%[^\n]s", key);
    int message_length = strlen(message), key_length = strlen(key);
    char temp_key[message_length], encrypted_message[message_length],
decrypted_message[message_length];
    for(count = 0, j = 0; count < message_length; ++count, ++j)
    {
        if(j == key_length)
        {
            j = 0;
        }
        temp_key[count] = key[j];
    }
    temp_key[count] = '\0';
    count = 0;
    while(count < message_length)
    {
        encrypted_message[count] = ((message[count] + temp_key[count]) % 26) + 'A';
        count = count + 1;
    }
    encrypted_message[count] = '\0';
    count = 0;
    while(count < message_length)
    {
        decrypted_message[count] = (((encrypted_message[count] - temp_key[count]) +
26) % 26) + 'A';
        count = count + 1;
    }
    decrypted_message[count] = '\0';
    printf("\n-------------------------------\n");
    printf("\nIntial String:\t%s", message);
    printf("\nKey:\t%s", key);
    printf("\nGenerated Key:\t%s", temp_key);
    printf("\nEncrypted Message:\t%s", encrypted_message);
    printf("\nDecrypted Message:\t%s", decrypted_message);
    return 0;
}
```

Output:

```
Message: CODINGALPHA
Key: XYZ
Generated Key: XYZXYZXYZXY
Encrypted Message: ZMCFLFXJOEY
```

Vigenere Cipher Decryption
Encrypted Messaged: ZMCFLFXJOEY
Generated Key: XYZXYZXYZXY
Decrypted Message: CODINGALPHA

5. ट्रांसपोजीशन विधि के लिए C प्रोग्रामः

```
#include<stdio.h>
#include<string.h>
void cipher(int i,int c);
int findMin();
void makeArray(int,int);
char arr[22][22],darr[22][22],emessage[111],retmessage[111],key[55];
char temp[55],temp2[55];
int k=0;
int main() {
        char *message,*dmessage;
        int i,j,klen,emlen,flag=0;
        int r,c,index,min,rows;
        clrscr();
        printf("Enetr the key\n");
        fflush(stdin);
        gets(key);
        printf("\nEnter message to be ciphered\n");
        fflush(stdin);
        gets(message);
        strcpy(temp,key);
        klen=strlen(key);
        k=0;
        for (i=0; ;i++) {
                if(flag==1)
                   break;
                for (j=0;key[j]!=NULL;j++) {
                        if(message[k]==NULL) {
                                flag=1;
                                arr[i][j]='-';
                        } else {
                                arr[i][j]=message[k++];
                        }
                }
        }
        r=i;
        c=j;
        for (i=0;i<r;i++) {
                for (j=0;j<c;j++) {
                        printf("%c ",arr[i][j]);
                }
```

```
            printf("\n");
    }
    k=0;
    for (i=0;i<klen;i++) {
            index=findMin();
            cipher(index,r);
    }
    emessage[k]='\0';
    printf("\nEncrypted message is\n");
    for (i=0;emessage[i]!=NULL;i++)
      printf("%c",emessage[i]);
    printf("\n\n");
    //deciphering
    emlen=strlen(emessage);
    //emlen is length of encrypted message
    strcpy(temp,key);
    rows=emlen/klen;
    //rows is no of row of the array to made from ciphered message
    rows;
    j=0;
    for (i=0,k=1;emessage[i]!=NULL;i++,k++) {
            //printf("\nEmlen=%d",emlen);
            temp2[j++]=emessage[i];
            if((k%rows)==0) {
                    temp2[j]='\0';
                    index=findMin();
                    makeArray(index,rows);
                    j=0;
            }
    }
    printf("\nArray Retrieved is\n");
    k=0;
    for (i=0;i<r;i++) {
            for (j=0;j<c;j++) {
                    printf("%c ",darr[i][j]);
                    //retrieving message
                    retmessage[k++]=darr[i][j];
            }
            printf("\n");
    }
    retmessage[k]='\0';
    printf("\nMessage retrieved is\n");
    for (i=0;retmessage[i]!=NULL;i++)
       printf("%c",retmessage[i]);
    getch();
    return(0);
```

```
}
void cipher(int i,int r) {
          int j;
          for (j=0;j<r;j++) { {
                              emessage[k++]=arr[j][i];
                    }
          }
          // emessage[k]='\0';
}
void makeArray(int col,int row) {
          int i,j;
          for (i=0;i<row;i++) {
                    darr[i][col]=temp2[i];
          }
}
int findMin() {
          int i,j,min,index;
          min=temp[0];
          index=0;
          for (j=0;temp[j]!=NULL;j++) {
                    if(temp[j]<min) {
                              min=temp[j];
                              index=j;
                    }
          }
          temp[index]=123;
          return(index);
}
```

Output:

```
          Enter the key
          Hello
          Enter the message to be ciphered
          how are you
          h o w   a
          r e   y o
          u - -  - -
          Encrypted message is
          oe-hruw - y-ao-

          Array Retrieved is
          h o w   a
          r e   y o
          u - -  - -
          Message retrieved is
          how are you
```

6. एफिन विधि के लिए C प्रोग्रामः

```
#include<stdio.h>
#include<string.h>
#include<ctype.h>
#include<stdlib.h>
int CalcGCD(int);
main()
{
 int i,j,k,gcd,alpha,beta,numstr[100],numcipher[100];
 char str[100],cipher[100];
 printf("Enter a string\n");
 gets(str);
 //converting entered string to Capital letters
 for(i=0,j=0;i<strlen(str);i++)
 {
  if(str[i]!=' ')
  {
   str[j]=toupper(str[i]);
   j++;
  }
  else
  {
   str[j]=' ';
   j++;
  }
 }
 str[j]='\0';
 printf("Entered string is : %s \n",str);
 printf("Enter Alpha value and must be between 1 and 25 both included\n");
 scanf("%d",&alpha);
 //Checking consitions
 if(alpha<1 || alpha>25)
 {
  printf("Alpha should lie in between 1 and 25\nSorry Try again !\n");
  exit(0);
 }
 gcd=CalcGCD(alpha);
 if(gcd!=1)
 {
  printf("gcd(alpha,26)=1 but \n gcd(%d,26)=%d\nSorry Try again !\n",alpha,gcd);
  exit(0);
 }
 printf("Enter Beta value and must be between 0 and 25 both included\n");
 scanf("%d",&beta);
 if(beta<0 || beta>25)
```

```
 {
  printf("Beta value should lie between 0 and 25\nSorry Try again !\n");
  exit(0);
 }
 //Conditions Over
 //Program Starts
 //Storing string in terms of ascii and to restore spaces I used -20
 for(i=0;i<strlen(str);i++)
{
  if(str[i]!=' ')
  numstr[i]=str[i]-'A';
  else
  numstr[i]=-20; }
 //Ciphering Process
    //If numcipher is more than 25 .We need to convert and ensure that lie in between 0
and 25.(indicating Alphabets)
    //A-0,B-1,C-2,.....Y-24,Z-25
    printf("Affine Cipher text is\n");
    for(i=0;i<strlen(str);i++)
    {
     if(numstr[i]!=-20)
     {
     numcipher[i]=((alpha*numstr[i])+beta)%26;
          printf("%c",(numcipher[i]+'A'));
     }
     else
     {
          printf(" ");
     }
    }
printf("\n");
}
int CalcGCD(int alpha)
{
 int x;
   int temp1=alpha;
   int temp2=26;
     while(temp2!=0)
      {
        x=temp2;
        temp2=temp1%temp2;
        temp1=x;
      }
     return(temp1);
}
```

Output:

Enter a String

```
kill him at dawn
Enter string is: KILL HIM AT DAWN
Enter Alpha value and must be between 1 and 25 both included
7
Enter Beta value and must be between 0 and 25 both included
2
Affine Cipher text is
UGBB ZGI CF XCAP
```

7. हिल विधि के लिए C प्रोग्रामः

```
#include<stdio.h>
#include<math.h>
float encrypt[3][1], decrypt[3][1], a[3][3], b[3][3], mes[3][1], c[3][3];
void encryption();        //encrypts the message
void decryption();        //decrypts the message
void getKeyMessage();  //gets key and message from user
void inverse();              //finds inverse of key matrix
void main() {
        getKeyMessage();
        encryption();
        decryption();
}
void encryption() {
        int i, j, k;

        for(i = 0; i < 3; i++)
                for(j = 0; j < 1; j++)
                        for(k = 0; k < 3; k++)
                                encrypt[i][j] = encrypt[i][j] + a[i][k] * mes[k][j];
        printf("\nEncrypted string is: ");
        for(i = 0; i < 3; i++)
                printf("%c", (char)(fmod(encrypt[i][0], 26) + 97));
}
void decryption() {
        int i, j, k;
        inverse();
        for(i = 0; i < 3; i++)
                for(j = 0; j < 1; j++)
                        for(k = 0; k < 3; k++)
                                decrypt[i][j] = decrypt[i][j] + b[i][k] * encrypt[k][j];
        printf("\nDecrypted string is: ");
        for(i = 0; i < 3; i++)
                printf("%c", (char)(fmod(decrypt[i][0], 26) + 97));

        printf("\n");
}
void getKeyMessage() {
```

```
        int i, j;
        char msg[3];
        printf("Enter 3x3 matrix for key (It should be inversible):\n");
        for(i = 0; i < 3; i++)
                for(j = 0; j < 3; j++) {
                        scanf("%f", &a[i][j]);
                        c[i][j] = a[i][j];
                }
        printf("\nEnter a 3 letter string: ");
        scanf("%s", msg);
        for(i = 0; i < 3; i++)
                mes[i][0] = msg[i] - 97;
}
void inverse() {
        int i, j, k;
        float p, q;

        for(i = 0; i < 3; i++)
                for(j = 0; j < 3; j++) {
                        if(i == j)
                                b[i][j]=1;
                        else
                                b[i][j]=0;}
        for(k = 0; k < 3; k++) {
                for(i = 0; i < 3; i++) {
                        p = c[i][k];
                        q = c[k][k];

                        for(j = 0; j < 3; j++) {
                                if(i != k) {
                                        c[i][j] = c[i][j]*q - p*c[k][j];
                                        b[i][j] = b[i][j]*q - p*b[k][j];
                                }}
                }}
        for(i = 0; i < 3; i++)
                for(j = 0; j < 3; j++)
                        b[i][j] = b[i][j] / c[i][i];
        printf("\n\nInverse Matrix is:\n");
        for(i = 0; i < 3; i++) {
                for(j = 0; j < 3; j++)
                        printf("%d ", b[i][j]);
                printf("\n");
        }}
```

Output:

```
        Enter 3x3 matrix for key (It should be inversible):
        6       24      1
```

```
13          16          10
20          17          15
Enter a 3 letter string: act
Encrypted string is: poh
Inverse Matrix is:
0.158730        - 0.777778        0.507937
0.011338        0.857143          -0.489796
-0.224490       0.857143          -0.489796
Decrypted string is: act
```

अभ्यास

1. सीजर या विस्थापन सिफर (कूटलेख) को समझाइए।
2. सरल प्रतिस्थापन सिफर (कूटलेख) से क्या समझते हैं?
3. मोनोअल्फाबेटिक और पॉलीअल्फाबेटिक सिफर (कूटलेख) की अवधारणा को स्पष्ट करें।
4. प्लेफेयर सिफर (कूटलेख) क्या है?
5. विगेनियर सिफर (कूटलेख) को उदाहरण के साथ समझाइए।
6. ट्रान्सपोजीशन सिफर (कूटलेख) से क्या समझते हैं?
7. एफिन सिफर (कूटलेख) को समझाइए।
8. निहिलिस्ट सिफर (कूटलेख) की अवधारणा को स्पष्ट करें।
9. प्रोडक्ट सिफर (कूटलेख) पर संक्षिप्त टिप्पणी लिखिए।
10. हिल सिफर (कूटलेख) क्या है?

अध्याय – 3

एन्क्रिप्शन स्टैंडर्ड
(कूटित मानक)

3.1 आधुनिक सिमेट्रिक की एन्क्रिप्शन (कूटित):

डिजिटल डेटा (अंकीय आँकड़ा) को अक्षरों के विपरीत बाइनरी अंकों (बिट्स) के स्ट्रिंग (रज्जु) के रूप में दर्शाया जाता है। आधुनिक क्रिप्टोसिस्टम (कूटतंत्र) को इस बाइनरी स्ट्रिंग को दूसरी बाइनरी स्ट्रिंग में परिवर्तित करने के लिए संसाधित करने की आवश्यकता होती है। इन बाइनरी स्ट्रिंग को कैसे संसाधित किया जाता है, इस पर आधारित, एक सममित एन्क्रिप्शन योजनाओं को निम्न प्रकारों में वर्गीकृत किया जा सकता है:

1. ब्लॉक सिफर (खण्ड कूटलेख):

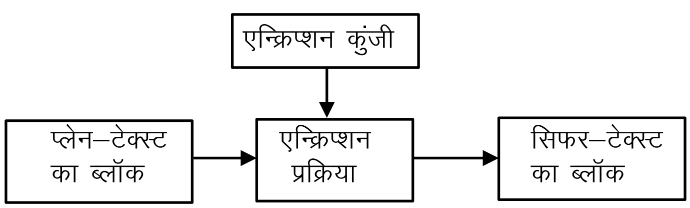
इस योजना में, प्लेन बाइनरी टेक्स्ट को बिट्स के ब्लॉक (खण्ड) में संसाधित किया जाता है, अर्थात् प्लेन–टेक्स्ट (साधारण–पाठ) बिट्स का एक ब्लॉक चयनित किया गया है, इस ब्लॉक पर सिफर–टेक्स्ट (कूटलेख–पाठ) बिट्स के ब्लॉक को उत्पन्न करने के लिए संक्रिया की एक श्रृंखला आयोजित की जाती है। ब्लॉक में बिट्स की संख्या निश्चित होती है। उदाहरण के लिए, योजनाएँ DES और AES में ब्लॉक का आकार क्रमशः 64 और 128 बिट्स का होता है।

2. स्ट्रीम सिफर (प्रवाह कूटलेख):

इस योजना में, प्लेन–टेक्स्ट (साधारण–पाठ) एक समय में एक बिट संसाधित करता है, अर्थात् प्लेन–टेक्स्ट (साधारण–पाठ) का एक बिट लिया जाता है, और एक बिट सिफर–टेक्स्ट (कूटलेख–पाठ) उत्पन्न करने के लिए संक्रिया की एक श्रृंखला निष्पादित की जाती है। तकनीकी रूप से, स्ट्रीम सिफर (प्रवाह कूटलेख) एक ब्लॉक सिफर (खण्ड कूटलेख) है जिसके ब्लॉक का आकार एक बिट होता है।

3.1.1 ब्लॉक सिफर (खण्ड कूटलेख):

ब्लॉक सिफर (खण्ड कूटलेख) की मूल योजना निम्नानुसार चित्रित की गई है:



(चित्र क्र0 3.1)

एक ब्लॉक सिफर (खण्ड कूटलेख) प्लेन–टेक्स्ट (कूटलेख–पाठ) बिट्स का एक ब्लॉक लेता है और सामान्यतः उसी आकार के सिफर–टेक्स्ट (कूटलेख–पाठ) बिट्स का एक ब्लॉक उत्पन्न करता है। दिए गए योजना में ब्लॉक का आकार निश्चित किया जाता है। ब्लॉक आकार का चयन सीधे एन्क्रिप्शन योजना की ताकत को प्रभावित नहीं करता है। सिफर (कूटलेख) की ताकत कुंजी लंबाई पर निर्भर करती है।

ब्लॉक आकार:

ब्लॉक का कोई भी आकार स्वीकार्य है, लेकिन ब्लॉक के आकार का चयन करते समय निम्नलिखित पहलुओं को ध्यान में रखा जाता है:

1. **बहुत छोटे ब्लॉक आकार से बचें** – माना ब्लॉक आकार m बिट्स है। तब संभावित प्लेन–टेक्स्ट बिट्स संयोजन 2^m है। यदि आक्रमणकर्ता कुछ समय पूर्व भेजे गए सिफर–टेक्स्ट ब्लॉक से संबंधित प्लेन–टेक्स्ट ब्लॉक को खोजता है, तो आक्रमणकर्ता उस एन्क्रिप्शन कुंजी का उपयोग करके भेजे गए प्लेन–टेक्स्ट/सिफर–टेक्स्ट युग्म का एक शब्दकोश बनाकर शब्दकोश आक्रमण आरंभ कर सकता है। एक बड़ा ब्लॉक आकार हमले को कठिन बनाता है क्योंकि शब्दकोश को बड़ा होना आवश्यक है।

2. **बहुत बड़ा ब्लॉक आकार न रखें** – बहुत बड़े ब्लॉक आकार के साथ, सिफर (कूटलेख) संचालित करने के लिए अक्षम हो जाता है। ऐसे प्लेन–टेक्स्ट (साधारण–पाठ) को एन्क्रिप्टेड (कूटित) होने से पहले पैडेड होने की आवश्यकता होगी।
3. **8 बिट के गुणक** – एक सुविधा युक्त ब्लॉक आकार 8 का गुणक होता है, क्योंकि यह कार्यान्वयन के लिए आसान है, जैसाकि अधिकांश कम्प्यूटर प्रोसेसर 8 बिट्स में डेटा को नियंत्रित करता है।

ब्लॉक सिफर में पैडिंगः

ब्लॉक सिफर निश्चित आकार के ब्लॉक को संसाधित करते हैं (माना 64 बिट्स)। प्लेन–टेक्स्ट (साधारण–पाठ) की लंबाई अधिकांशतः ब्लॉक आकार का गुणक नहीं होता है। उदाहरण के लिए, 150–बिट प्लेन–टेक्स्ट (साधारण–पाठ) प्रत्येक 64 बिट्स के दो ब्लॉक प्रदान करता है और तृतीय ब्लॉक में शेष 22 बिट्स होती हैं। बिट्स के अंतिम ब्लॉक को अनावश्यक जानकारी के साथ पैड की आवश्यकता है ताकि योजना के ब्लॉक आकार के बराबर अंतिम ब्लॉक की लंबाई हो सके। हमारे उदाहरण में, शेष 22 बिट्स को एक पूर्ण ब्लॉक प्रदान करने के लिए अतिरिक्त 42 अनावश्यक बिट्स जोड़ने की आवश्यकता है। अंतिम ब्लॉक में बिट्स जोड़ने की प्रक्रिया को पैडिंग के रूप में जाना जाता है।

बहुत अधिक पैडिंग प्रणाली को अक्षम बनाता है। इसके अतिरिक्त, पैडिंग प्रणाली को असुरक्षित रूप से प्रस्तुत कर सकता है, अगर पैडिंग को सदैव समान बिट्स के साथ किया जाता है।

ब्लॉक सिफर योजनाएँः

ब्लॉक सिफर योजनाओं की एक बड़ी संख्या है जो उपयोग में हैं। उनमें से कई सार्वजनिक रूप से ज्ञात हैं। सबसे लोकप्रिय और प्रमुख ब्लॉक सिफर नीचे सूचीबद्ध हैं।

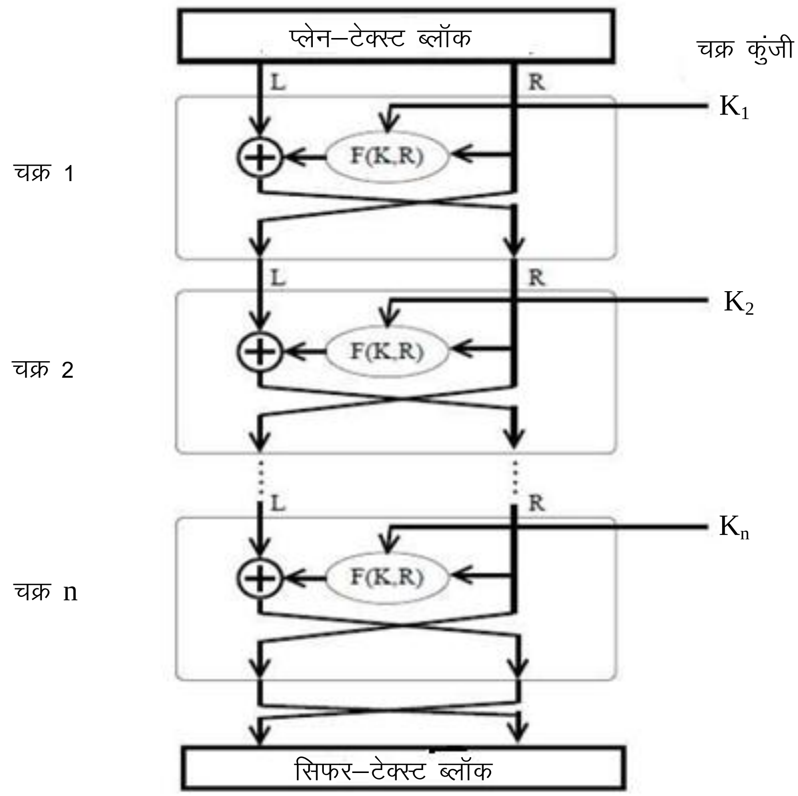
1. **डाटा एन्क्रिप्शन स्टैंडर्ड (DES)** (आँकड़ा कूटित मानक) – 1990 के दशक का लोकप्रिय ब्लॉक सिफर। इसे अब खंडित ब्लॉक सिफर माना जाता है, मुख्य रूप से इसके छोटे आकार के कारण।
2. **ट्रिपल डीईएस** (त्रिक डीईएस) – यह बार–बार DES अनुप्रयोगों के आधार पर एक संस्करण योजना है। यह अभी भी एक सम्मानित ब्लॉक सिफर है लेकिन उपलब्ध नए तेज ब्लॉक सिफर की तुलना में अक्षम है।
3. **एडवांस्ड एन्क्रिप्शन स्टैंडर्ड (AES)** (उन्नत कूटित मानक) – यह एक अपेक्षाकृत नया ब्लॉक सिफर है जो एन्क्रिप्शन एल्गोरिथम Rijndael पर आधारित है जिसने AES डिजाइन प्रतियोगिता जीती थी।
4. IDEA – यह 64 बिट्स के ब्लॉक आकार और 128 बिट्स की कुंजी आकार के साथ पर्याप्त मजबूत ब्लॉक सिफर (खण्ड कूटलेख) है। बहुत सारे अनुप्रयोग IDEA एन्क्रिप्शन का उपयोग करते हैं, जिसमें Pretty Good Privacy (PGP) प्रोटोकॉल (संदेशाचार) के प्रारंभिक संस्करण शामिल हैं।
5. Twofish – ब्लॉक सिफर (खण्ड कूटलेख) की यह योजना 128 बिट्स के ब्लॉक आकार और परिवर्तनीय लंबाई की कुंजी का उपयोग करती है। यह AES प्रतियोगिता में से एक था। यह 64 बिट्स के ब्लॉक आकार के साथ पहले ब्लॉक सिफर ब्लोफिश पर आधारित है।
6. Serpent – 128 बिट्स के ब्लॉक आकार और 128, 192 या 256 बिट्स की कुंजी लंबाई के साथ एक ब्लॉक सिफर (खण्ड कूटलेख), जो AES प्रतियोगिता में से एक था। यह धीमा है लेकिन अन्य ब्लॉक सिफर (खण्ड कूटलेख) की तुलना में अधिक सुरक्षित डिजाइन है।

फीस्टल ब्लॉक सिफरः

फीस्टल सिफर ब्लॉक सिफर की एक विशिष्ट योजना नहीं है। यह एक अभिकल्पना प्रारूप है जिसमें से कई अलग–अलग ब्लॉक सिफर (खण्ड कूटलेख) व्युत्पन्न होते हैं। DES फीस्टल सिफर का सिर्फ एक उदाहरण है। फीस्टल सिफर संरचना के आधार पर एक क्रिप्टोग्राफिक (कूटलेखीय) प्रणाली एन्क्रिप्शन और डिक्रिप्शन दोनों के लिए समान एल्गोरिथम (कलनविधि) का उपयोग करती है।

एन्क्रिप्शन प्रक्रियाः

एन्क्रिप्शन प्रक्रिया फीस्टल संरचना का उपयोग करती है जिसमें प्लेन–टेक्स्ट (साधारण–पाठ) के प्रसंस्करण के कई चक्र शामिल होते हैं, प्रत्येक चरण में एक 'प्रतिस्थापन' चरण होता है जिसके बाद क्रमपरिवर्तन चरण होता है। फीस्टल संरचना को निम्नलिखित चित्र में दिखाया गया है –



(चित्र क्र0 3.2)

- प्रत्येक चक्र में इनपुट ब्लॉक को दो भागों में बांटा गया है, जिसे बायां आधा और दायां आधा के रूप में रखा गया है और इन भागों को क्रमशः L और R के रूप में दर्शाया जा सकता है।
- प्रत्येक चक्र में, ब्लॉक का दायां आधा भाग R अपरिवर्तित रहता है। लेकिन बायां आधा भाग L एक संक्रिया के माध्यम से चलता है जो R और एन्क्रिप्शन कुंजी पर निर्भर करता है। सबसे पहले, हम एक एन्क्रिप्टिंग फलन F लागू करते हैं जिसमें दो इनपुट होते हैं – एक कुंजी K और R। फलन आउटपुट F(K, R) जनित करता है। तत्पश्चात् हम आउटपुट प्राप्त करने के लिए फलन F(K, R) और L के साथ XOR संक्रिया करते हैं।
- प्रत्येक चक्र के समय पूरी एन्क्रिप्शन कुंजी का उपयोग करने के स्थान पर, DES जैसे फीस्टल सिफर के वास्तविक कार्यान्वयन में, एक गोल–निर्भर कुंजी (एक उपकुंजी) एन्क्रिप्शन कुंजी से जनित की जाती है। इसका अर्थ है कि प्रत्येक चक्र एक अलग कुंजी का उपयोग करता है, हालांकि ये सभी उपकुंजी मूल कुंजी से संबंधित होती हैं।
- प्रत्येक चक्र के अंत में क्रमपरिवर्तन चरण संशोधित L और असंशोधित R का आपस में विनिमय करता है। इसलिए, वर्तमान चक्र का R अगले चक्र का L होगा और अगले चक्र के लिए R वर्तमान चक्र का आउटपुट L होगा।
- प्रतिस्थापन और क्रमपरिवर्तन चरण चक्र बनाते हैं। चक्रों की संख्या एल्गोरिथम डिजाइन द्वारा निर्दिष्ट की जाती है।

- एक बार अंतिम चक्र पूरा हो जाने के उपरान्त सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक बनाने के लिए दो सब–ब्लॉक R और L को एक क्रम से श्रेणीबद्व किया जाता है।

फीस्टल सिफर डिजाइन करने का कठिन भाग राउंड फंक्शन (चक्र फलन) F का चयन है। अखंडित योजना होने के लिए, इस फंक्शन में कई महत्वपूर्ण गुण होने चाहिए।

डिक्रिप्शन प्रक्रियाः

फीस्टेल सिफर में डिक्रिप्शन की प्रक्रिया लगभग एन्क्रिप्शन के समान ही है। प्लेन–टेक्स्ट (साधारण–पाठ) के ब्लॉक से आरंभ करने के स्थान पर, सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को फीस्टल संरचना के आरंभ में रखा जाता है और फिर उसके बाद की प्रक्रिया दिए गए चित्र में वर्णित जैसा ही है।

प्रक्रिया लगभग समान होती है और बिल्कुल वही नहीं होती है। डिक्रिप्शन की स्थिति में केवल अंतर यह है कि एन्क्रिप्शन में उपयोग की जाने वाली उपकुंजियों को विपरीत क्रम में उपयोग किया जाता है।

फीस्टल सिफर के अंतिम चरण में L और R की अंतिम स्वैपिंग (आपस में बदलना) आवश्यक है। यदि इन्हें स्वैप नहीं किया गया है तो परिणामस्वरूप सिफर–टेक्स्ट (कूटलेख–पाठ) को उसी एल्गोरिथम (कलनविधि) का उपयोग करके डिक्रिप्ट (अकूटित) नहीं किया जा सकता।

चक्रों की संख्याः

फीस्टल सिफर में उपयोग किए जाने वाले चक्रों की संख्या प्रणाली से वांछित सुरक्षा पर निर्भर करती है। चक्रों की अधिक संख्या अधिक सुरक्षित प्रणाली प्रदान करती है। लेकिन साथ ही, अधिक चक्र का अर्थ मंद एन्क्रिप्शन और डिक्रिप्शन प्रक्रिया। प्रणाली में चक्रों की संख्या इस प्रकार दक्षता–सुरक्षा पर निर्भर करती है।

3.1.2 स्ट्रीम सिफर (प्रवाह कूटलेख):

एक स्ट्रीम सिफर (प्रवाह कूटलेख) एक एन्क्रिप्शन एल्गोरिथम (कलनविधि) है जो एक समय में प्लेन–टेक्स्ट (साधारण–पाठ) के 1 बिट या बाइट को एन्क्रिप्ट (कूटित) करता है। यह कुंजी के रूप में छद्म यादृच्छिक बिट्स के एक अनंत प्रवाह का उपयोग करता है। स्ट्रीम सिफर (प्रवाह कूटलेख) को कार्यान्वयन के लिए सुरक्षित रहने हेतु, इसके छद्म यादृच्छिक जनक को अप्रत्याशित होना चाहिए और कुंजी का पुनः उपयोग नहीं किया जाना चाहिए। स्ट्रीम सिफर (प्रवाह कूटलेख) को एक आदर्शीकृत सिफर (कूटलेख) का अनुमान लगाने के लिए डिजाइन किया गया है, जिसे वन–टाइम पैड के नाम से जाना जाता है।

वन–टाइम पैड, जो पूरी तरह से यादृच्छिक कुंजी को नियोजित करने वाला है, संभावित रूप से पूर्ण गोपनीयता प्राप्त कर सकता है। अर्थात् इसे ब्रूट फोर्स आक्रमण के प्रति पूरी तरह से प्रतिरक्षित होना चाहिए। वन–टाइम पैड के साथ समस्या यह है कि, इस तरह के एक सिफर (कूटलेख) बनाने के लिए, इसकी कुंजी प्लेन–टेक्स्ट (साधारण–पाठ) से लंबी या उससे अधिक लंबी होनी चाहिए। अन्य शब्दों में, यदि हमारे पास 500 मेगाबाइट वीडियो फाइल है जिसे हम एन्क्रिप्ट (कूटित) करना चाहते हैं, तो हमें कम से कम 4 गिगाबिट्स की एक कुंजी की आवश्यकता होगी।

स्पष्ट है, जबकि शीर्ष गुप्त जानकारी या राष्ट्रीय सुरक्षा की स्थिति वन–टाइम पैड के उपयोग का अधिपत्र दे सकते हैं, ऐसे सिफर दिन–प्रतिदिन सार्वजनिक उपयोग के लिए बहुत अव्यवहारिक होंगे। एक स्ट्रीम सिफर (प्रवाह कूटलेख) की कुंजी अब तक मूल संदेश के रूप में नहीं है। इसलिए, यह अब पूर्ण गोपनीयता का अधिपत्र नहीं दे सकता है। हालांकि, यह अभी भी एक मजबूत स्तर की सुरक्षा प्राप्त कर सकता है।

लोकप्रिय स्ट्रीम सिफर (प्रवाह कूटलेख):

RC4, जिसका अर्थ रिवेस्ट सिफर 4 है, सभी स्ट्रीम सिफर (प्रवाह कूटलेख) में से सबसे अधिक उपयोग किया जाता है, विशेष रूप से सॉफ्टवेयर में। इसे ARCFOUR या ARC4 के रूप में भी जाना जाता है।

RC4 का उपयोग विभिन्न प्रोटोकॉल जैसे WEP और WPA (दोनों वायरलेस नेटवर्क के लिए सुरक्षा प्रोटोकॉल हैं) के साथ–साथ TLS में किया जाता है। दुर्भाग्यवश, हाल के अध्ययनों ने RC4 की कमजोरियों को प्रकाशित किया है, जिससे मोजिला और माइक्रोसॉफ्ट को यह सलाह देने के लिए प्रेरित किया जाता है कि जहाँ संभव हो इसे असमर्थ करें। वास्तव में, RFC 7465, TLS के सभी संस्करणों में RC4 के उपयोग को प्रतिबंधित करता है।

इन निष्कर्षों ने निश्चित रूप से अन्य स्ट्रीम सिफर (प्रवाह कूटलेख) (जैसे SALSA, SOSEMANUK, PANAMA और कई अन्य जो पहले से उपलब्ध हैं लेकिन कभी भी RC4 के समान लोकप्रियता प्राप्त नहीं कर पाये) को उभरने और संभवतः अपनी जगह लेने की अनुमति मिलेगी।

एक स्ट्रीम सिफर (प्रवाह कूटलेख) एक सममित कुंजी सिफर है जहाँ प्लेन–टेक्स्ट (साधारण–पाठ) अंक को छद्म यादृच्छिक सिफर (कूटलेख) को डिजिट स्ट्रीम (अंक प्रवाह) के साथ संयोजित किया जाता है। एक स्ट्रीम सिफर (प्रवाह कूटलेख) में, सिफर–टेक्स्ट (कूटलेख–पाठ) प्रवाह का एक अंक प्राप्त करने के लिए प्रत्येक प्लेन–टेक्स्ट (साधारण–पाठ) अंक संगत कीस्ट्रीम (कुंजी प्रवाह) अंक के साथ एक समय में एक बार एन्क्रिप्टेड (कूटित) किया जाता है। चूंकि प्रत्येक अंक का एन्क्रिप्शन सिफर (कूटलेख) की वर्तमान स्थिति पर निर्भर है, इसलिए इसे स्टेट सिफर भी कहा जाता है। एक अंक सामान्यतः एक बिट होता है और संयोजन ऑपरेशन XOR होता है।

छद्म यादृच्छिक कीस्ट्रीम (कुंजी प्रवाह) सामान्यतः डिजिटल शिफ्ट रजिस्टर्स का उपयोग करके यादृच्छिक बीज मान से क्रमशः उत्पन्न होता है। बीज मान सिफर–टेक्स्ट (कूटलेख–पाठ) प्रवाह को डिक्रिप्ट (अकूटित) करने के लिए क्रिप्टोग्राफिक (कूटलेखीय) कुंजी के रूप में कार्य करता है। स्ट्रीम सिफर (प्रवाह कूटलेख), ब्लॉक सिफर (खण्ड कूटलेख) से सममित एन्क्रिप्शन के लिए एक अलग दृष्टिकोण का प्रतिनिधित्व करते हैं। ब्लॉक सिफर (खण्ड कूटलेख) एक निश्चित, असंगत परिवर्तन के साथ अंक के बड़े ब्लॉक पर काम करते हैं। यह भेद हमेशा स्पष्ट नहीं होता है। संक्रिया की कुछ विधियों में, ब्लॉक सिफर (खण्ड कूटलेख) का उपयोग इसप्रकार से किया जाता है कि यह एक स्ट्रीम सिफर (प्रवाह कूटलेख) के रूप में प्रभावी रूप से कार्य करे।

स्ट्रीम सिफर (प्रवाह कूटलेख) आमतौर पर ब्लॉक सिफर (खण्ड कूटलेख) की तुलना में उच्च गति पर निष्पादित होते हैं और कम हार्डवेयर जटिलता रखते हैं। हालांकि, अगर गलत तरीके से उपयोग किया जाता है तो स्ट्रीम सिफर (प्रवाह कूटलेख) गंभीर सुरक्षा समस्याओं के लिए अतिसंवेदनशील हो सकते हैं। विशेष रूप से, समान प्रारंभिक अवस्था का दो बार उपयोग नहीं किया जाना चाहिए। स्ट्रीम सिफर (प्रवाह कूटलेख) को एक सिद्ध अखंडित सिफर, वन–टाइम पैड की क्रिया को अनुमानित करने के रूप में देखा जा सकता है, जिसे कभी–कभी वर्नम सिफर के नाम से भी जाना जाता है। वन–टाइम पैड पूरी तरह से यादृच्छिक अंकों की एक कीस्ट्रीम (कुंजी प्रवाह) का उपयोग करता है।

सिफर–टेक्स्ट (कूटलेख–पाठ) बनाने के लिए कीस्ट्रीम (कुंजी प्रवाह) को प्लेन–टेक्स्ट (साधारण–पाठ) अंकों के साथ जोड़ा जाता है। यह प्रणाली क्लाउड ई. शैनन द्वारा 1949 में सुरक्षित साबित हुई थी। हालांकि, कीस्ट्रीम (कुंजी प्रवाह) को कम से कम समान लंबाई के साथ यादृच्छिक रूप से जनित किया जाना चाहिए और इसे एक से अधिक बार उपयोग नहीं किया जा सकता है। यह प्रणाली को कई व्यावहारिक अनुप्रयोगों में लागू करने के लिए दुष्कर बनाता है, और परिणामतः, एक महत्वपूर्ण पैड का व्यापक रूप से उपयोग नहीं किया जाता है, सबसे महत्वपूर्ण अनुप्रयोगों को छोड़कर। ऐसे अनुप्रयोगों के लिए कुंजी का उत्पादन, वितरण और प्रबंधन महत्वपूर्ण हैं।

एक स्ट्रीम सिफर (प्रवाह कूटलेख) 128 बिट्स जैसी बहुत छोटी और अधिक सुविधाजनक कुंजी का उपयोग करता है। इस कुंजी के आधार पर, यह एक छद्म यादृच्छिक कुंजीस्ट्रीम (कुंजी प्रवाह) उत्पन्न करता है जिसे प्लेन–टेक्स्ट (साधारण–पाठ) अंकों के साथ एक ही समय में एक ही समय में जोड़ा जा सकता है। हालांकि, यह एक लागत पर आता है। कीस्ट्रीम (कुंजी प्रवाह) अब छद्म यादृच्छिक है और इसलिए वास्तव में यादृच्छिक नहीं है। वन–टाइम पैड से जुड़े सुरक्षा का प्रमाण अधिक समय तक नहीं रखता है। स्ट्रीम सिफर (प्रवाह कूटलेख) के पूरी तरह से असुरक्षित होने के लिए यह पर्याप्त संभव है।

एक स्ट्रीम सिफर (प्रवाह कूटलेख) एक आंतरिक अवस्था के आधार पर कीस्ट्रीम (कुंजी प्रवाह) के उतरोत्तर अवयवों को उत्पन्न करता है। इस अवस्था को अनिवार्य रूप से दो विधियों द्वारा अद्यतन किया जाता है। यदि प्लेन–टेक्स्ट (साधारण–पाठ) या सिफर–टेक्स्ट (कूटलेख–पाठ) संदेशों की अवस्था स्वतंत्र रूप से बदलती है, तो सिफर को सिंक्रोनस स्ट्रीम सिफर के रूप में वर्गीकृत किया जाता है।

इसके विपरीत, पिछले सिफर–टेक्स्ट (कूटलेख–पाठ) अंकों के आधार पर सेल्फ–सिंक्रनाइज स्ट्रीम सिफर अपनी अवस्था को अद्यतन करते हैं।

सिंक्रोनस स्ट्रीम सिफर (प्रवाह कूटलेख):

सिंक्रोनस स्ट्रीम सिफर में छद्म–यादृच्छिक अंकों का एक प्रवाह प्लेन–टेक्स्ट (साधारण–पाठ) और सिफर–टेक्स्ट (कूटलेख–पाठ) संदेशों से स्वतंत्र रूप से उत्पन्न होता है, और फिर प्लेन–टेक्स्ट (एन्क्रिप्ट करने के लिए) या सिफर–टेक्स्ट (डिक्रिप्ट करने के लिए) के साथ मिलता है।

सामान्यतः, बाइनरी अंकों का उपयोग किया जाता है (बिट्स), और कीस्ट्रीम को XOR संक्रिया का उपयोग करके प्लेन–टेक्स्ट (साधारण–पाठ) के साथ संयोजित किया जाता है। इसे एक बाइनरी एडेटिव स्ट्रीम सिफर (बाइनरि योग प्रवाह कूटलेख) भी कहा जाता है।

यदि जोड़े गये या खोए जाने के स्थान पर ट्रांसमिशन में एक अंक दूषित हो जाता है, तो प्लेन–टेक्स्ट (साधारण–पाठ) में केवल एक अंक प्रभावित होता है और त्रुटि संदेश के अन्य हिस्सों में प्रवाहित नहीं होती है। ट्रांसमिशन त्रुटि दर उच्च होने पर यह प्रगुण उपयोगी होता है। हालांकि, यह कम संभावना है कि बिना किसी तंत्र के त्रुटि का पता लगाया जाएगा। इसके अतिरिक्त, इस प्रगुण के कारण, सिंक्रोनस स्ट्रीम सिफर सक्रिय आक्रमण के लिए बहुत संवेदनशील हैं। यदि कोई आक्रमणकर्ता सिफर–टेक्स्ट (कूटलेख–पाठ) में एक अंक बदल सकता है, तो वह इसी प्लेन–टेक्स्ट (साधारण–पाठ) में अनुमानित परिवर्तन करने में सक्षम हो सकता है। उदाहरण के लिए, सिफर–टेक्स्ट (कूटलेख–पाठ) में थोड़ा सा झटका देने से प्लेन–टेक्स्ट (साधारण–पाठ) में झटका दिया जा सकता है।

सेल्फ–सिंक्रनाइजिंग स्ट्रीम सिफरः

एक और दृष्टिकोण कीस्ट्रीम (कुंजी प्रवाह) की गणना करने के लिए पिछले N सिफर–टेक्स्ट (कूटलेख–पाठ) अंकों में से कई का उपयोग करता है। ऐसी योजनाएं सेल्फ–सिंक्रनाइजिंग स्ट्रीम सिफर, एसिंक्रोनस स्ट्रीम सिफर या सिफर–टेक्स्ट (कूटलेख–पाठ) ऑटोकी के रूप में जानी जाती हैं। सेल्फ–सिंक्रनाइजेशन का विचार 1946 में पेटेंट किया गया था, और इसका लाभ यह है कि प्राप्तकर्ता स्वचालित रूप से N सिफर–टेक्स्ट (कूटलेख–पाठ) अंकों को प्राप्त करने के उपरान्त कीस्ट्रीम (कुंजी प्रवाह) जनक के साथ सिंक्रनाइज हो जाएगा। ऐसा करने से, यदि अंकों को गिरा दिया जाता है या संदेश प्रवाह में जोड़ा जाता है, तो उनकी पुनः प्राप्ति आसान हो जाती है। एकल–अंक त्रुटियां उनके प्रभाव में सीमित हैं, केवल N प्लेन–टेक्स्ट (साधारण–पाठ) अंकों तक प्रभावित करती हैं।

सिंक्रनाइजिंग स्ट्रीम सिफर का एक उदाहरण सिफर फीडबैक मोड (CFB) में एक ब्लॉक सिफर (खण्ड कूटलेख) है।

3.2 डाटा एन्क्रिप्शन स्टैंडर्ड (आँकड़ा कूटित मानक):

1972 में, नेशनल इंस्टीट्यूट ऑफ स्टैंडर्ड एंड टेक्नोलॉजी (NIST), जिसे नेशनल ब्यूरो ऑफ स्टैंडर्ड्स नाम से जाना जाता है, ने क्रिप्टोग्राफिक एल्गोरिथम (कूटलेखीय कलनविधि) के प्रस्तावों का अनुरोध किया जो अवर्गीकृत जानकारी की रक्षा के लिए उपयोग किए जा सकते थे। वे चाहते थे कि एल्गोरिथम (कलनविधि) बहुत सुरक्षित हो, सस्ती, समझने में आसान और विभिन्न अनुप्रयोगों के लिए अनुकूलनीय ताकि विभिन्न संस्थानों और सामान्य व्यक्तियों द्वारा एल्गोरिथम (कलनविधि) का उपयोग किया जा सके।

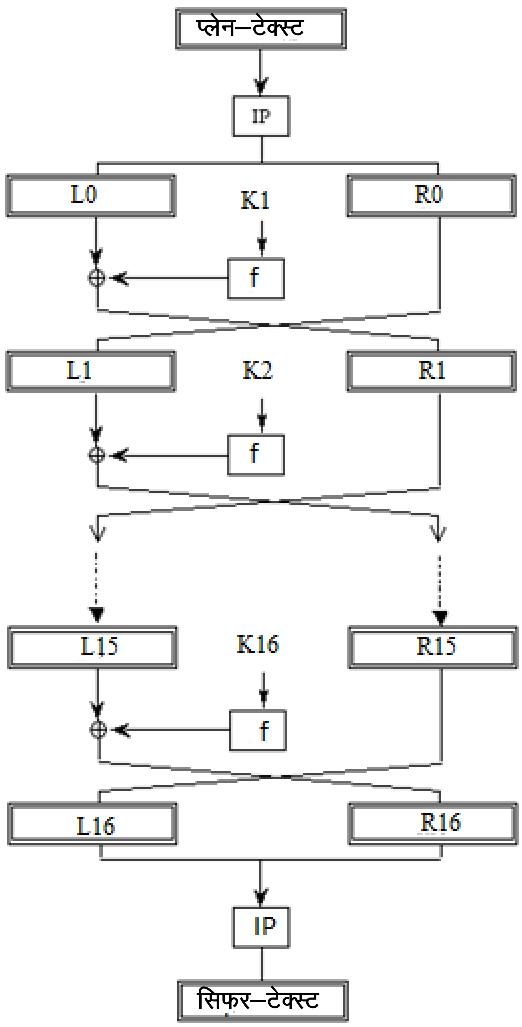
1974 में उन्होंने फिर से अनुरोध किया क्योंकि उन्हें 1972 में कोई व्यवहार्य प्रस्ताव नहीं मिला था। इस बार आईबीएम ने लूसिफर एल्गोरिथम (कलनविधि) प्रस्तुत किया था। एल्गोरिथम (कलनविधि) को अपनी सुरक्षा का मूल्यांकन करने के लिए राष्ट्रीय सुरक्षा एजेंसी (NSA) को भेजा गया था। NSA ने 56–बिट कुंजी के साथ एक 128–बिट कुंजी के प्रतिस्थापन के रूप में सबसे महत्वपूर्ण व्यक्ति के साथ एल्गोरिथम (कलनविधि) में कुछ संशोधन किए।

बहुत से व्यक्तियों को संदेह था कि NSA द्वारा किए गए संशोधन एल्गोरिथम (कलनविधि) को कमजोर बनाने और पीछे के दरवाजे को जोड़ने के लिए जानबूझकर थे ताकि उसके एजेंट कुंजी के बिना एन्क्रिप्टेड संदेशों को डिक्रिप्ट कर सकें। इस तरह के संदेहों को नजरअंदाज करते हुए, NIST ने संशोधित एल्गोरिथम (कलनविधि) को नवंबर 1976 में एक संघीय मानक के रूप में अपनाया।

एल्गोरिथम (कलनविधि) का नाम डेटा एन्क्रिप्शन मानक में बदल दिया गया और जनवरी 1977 में FIPS PUB 46 के रूप में प्रकाशित किया गया। तब से यह विभिन्न अनुप्रयोगों के लिए व्यापक रूप से उपयोग किया जाने वाला क्रिप्टोग्राफिक एल्गोरिथम (कूटलेखीय कलनविधि) रहा है, और संदेह धीरे–धीरे खत्म हो गए क्योंकि कोई भी DES पर आक्रमण करने के लिए त्रुटि नहीं ढूंढ पाया।

पिछले कुछ वर्षों में, कम्प्यूटर अधिक शक्तिशाली हो गए हैं और DES पर विभिन्न ब्रूट–फोर्स आक्रमणों ने अपनी क्षमताओं को एक शक्तिशाली और सुरक्षित क्रिप्टोसिस्टम (कूटतंत्र) के रूप में कमजोर कर दिया है। 1997 में, NIST ने संघीय मानक के रूप में DES के आधिकारिक समर्थन को त्याग दिया और उन्नत एन्क्रिप्शन मानक नामक एक नए एल्गोरिथम (कलनविधि) पर काम करना आरंभ किया।

DES **एल्गोरिथम (कलनविधि):**



(चित्र क्र0 3.3)

ब्लॉक आकार: DES में, 64 बिट्स के ब्लॉक पर एन्क्रिप्शन/डिक्रिप्शन किया जाता है। प्लेन–टेक्स्ट/सिफर–टेक्स्ट को 64 बिट्स के ब्लॉक में विभाजित किया जाता है और प्रत्येक ब्लॉक पर एल्गोरिथम (कलनविधि) लागू होता है।

कुंजीः कुंजी में 56 बिट हैं, लेकिन 64 बिट्स की स्ट्रिंग के रूप में व्यक्त किया जाता है। 8वीं, 16वीं, 24वीं, ..., बिट्स समता बिट्स हैं, जो इसप्रकार से व्यवस्थित होती हैं कि 8 बिट्स का प्रत्येक ब्लॉक 1's का एक विषम संख्या रखे। यह कुंजी में त्रुटि का पता लगाने के लिए होता है।

एल्गोरिदमः 64 बिट्स के एक प्लेन–टेक्स्ट (साधारण–पाठ) m के साथ आरंभ करें।

1. $m_0 = IP(m)$ को प्राप्त करने के लिए m के बिट्स को एक निश्चित प्रारंभिक क्रमपरिवर्तन द्वारा क्रम परिवर्तित किया जाता है। अब माना $m_0 = L_0R_0$, जहां L_0, m_0 का प्रथम 32 बिट्स है और R_0, m_0 अंतिम 32 बिट्स है।

2. $1 \leq I \leq 16$ के लिए निम्न करें:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i),$$

जहाँ K_i कुंजी K से प्राप्त 48 बिट्स की स्ट्रिंग है और f एक फलन है जिसे बाद में वर्णित किया जायेगा।

3. $R_{16}L_{16}$ प्राप्त करने के लिए बायें और दायें भागों का आपस में विनिमय करें, फिर सिफर (कूटलेख) परीक्षण प्राप्त करने के लिए प्रारंभिक क्रमपरिवर्तन के व्युत्क्रम को लागू करें

$$c = IP^{-1}(R_{16}L_{16}).$$

प्रारंभिक क्रमपरिवर्तनः प्रारंभिक क्रमपरिवर्तन, जिसमें कोई क्रिप्टोग्राफिक (कूटलेखीय) महत्व नहीं है, लेकिन जो शायद 1970 के दशक में उपलब्ध चिप्स में एल्गोरिथम (कलनविधि) लोड को अधिक कुशलतापूर्वक बनाने के लिए अभिकल्पित किया गया था, को प्रारंभिक क्रमपरिवर्तन तालिका द्वारा वर्णित किया जाता है। इसका अर्थ है कि m का 58वां बिट m_0 का प्रथम बिट बन जाता है, m का 50वां बिट m_0 का दूसरा बिट बन जाता है।

प्रारंभिक क्रमपरिवर्तन तालिकाः

58	50	42	34	26	18	19	2
60	52	44	36	26	28	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

कुंजी क्रमपरिवर्तनः

1. समता बिट्स को त्याग दिया जाता है और शेष बिट्स का निम्न तालिका द्वारा क्रम परिवर्तित किया जाता है।

कुंजी क्रमपरिवर्तन तालिकाः

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15

7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

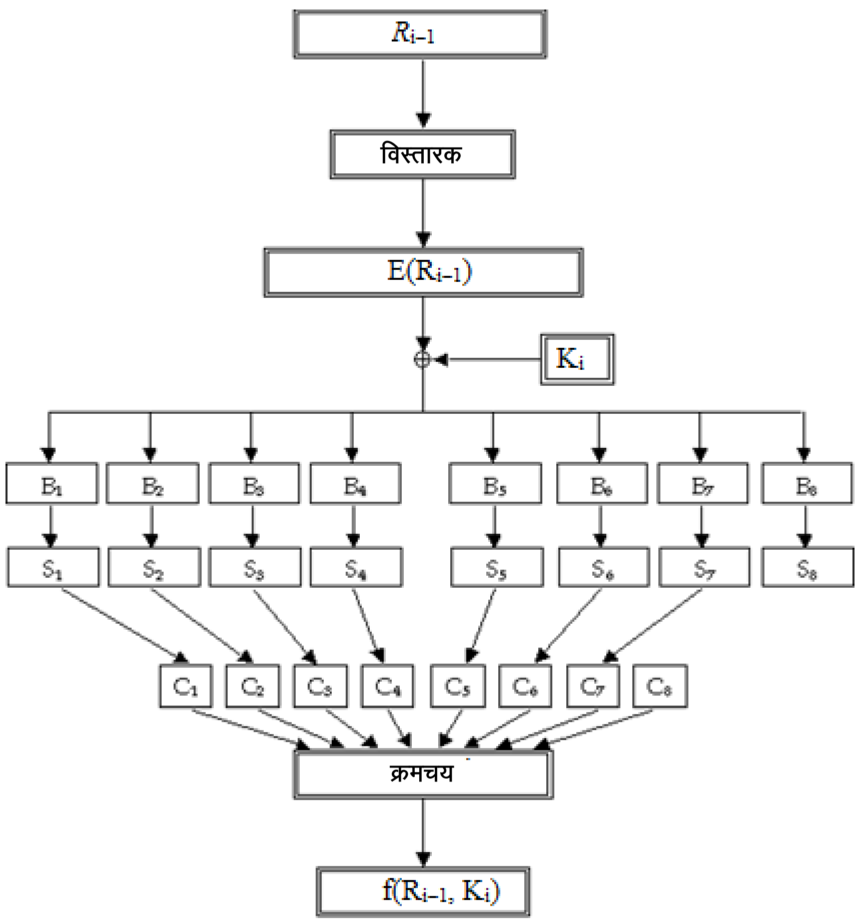
परिणाम को C_0D_0 के रूप में लिखें, जहां C_0 और D_0 28 बिट्स रखते हैं।

2. $1 \leq I \leq 16$ के लिए माना $C_i = LS_i(C_{i-1})$ और $D_i = LS_i(D_{i-1})$। यहाँ LS_i का अर्थ है, निम्नलिखित तालिका के अनुसार इनपुट को एक या दो स्थान बाईं ओर स्थानांतरित करें।

प्रति चक्र स्थानांतरित कुंजी बिट्स की संख्याः

चक्र	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
विस्थापन	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3.



(चित्र क्र0 3.4)

फलन $f(R_{i-1},K_i)$: ऊपर दिए गए चित्र में चित्रित फलन $f(R_{i-1}, K_i)$ कई चरणों में वर्णित है।

निम्न तालिका के अनुसार 56–बिट स्ट्रिंग C_iD_i से 48 बिट्स चुनें। आउटपुट K_i है।

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

विस्तार क्रम परिवर्तन:

1. सर्वप्रथम, R को निम्नलिखित तालिका द्वारा E (R) में विस्तारित किया जाता है। इसका अर्थ है कि E (R) का प्रथम बिट R का 32वां बिट है, इत्यादि। स्मरण रहे E (R) में 48 बिट हैं।

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	31	1

2. E (R) Å K_i की गणना करें, जिसमें 48 बिट्स हैं, और $B_1B_2\ldots B_8$ के रूप में लिखें, जहां प्रत्येक B_j 6 बिट रखता है।

3. यहाँ 8 S–बॉक्स $S_1,\ldots,S_8$ हैं। यहाँ B_j, S_j के लिए इनपुट है। $B_j = b_1b_2\ldots.b_6$ लिखें। S–बॉक्स की पंक्ति b_1b_6 द्वारा उल्लेखित की जाती है जबकि $b_2b_3b_4b_5$ स्तम्भ को निर्धारित करता है। उदाहरण के लिए यदि $B_4 = 001001$, तो पंक्ति 01 (दूसरी पंक्ति) और कॉलम 0100 (5 वें कॉलम) देखें। इस चरण से प्रत्येक S–बॉक्स के लिए प्राप्त आउटपुट 4 बिट होगा और हम आठ 4–बिट आउटपुट $C_1, C_2\ldots C_8$ प्राप्त करेंगे।

4. स्ट्रिंग $C_1, C_2\ldots C_8$ निम्नलिखित तालिका के अनुसार क्रम परिवर्तित करते है।

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

परिणामी 32–बिट स्ट्रिंग f (R, K_i) है।

S–बॉक्स 1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S–बॉक्स 2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S–बॉक्स 3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S–बॉक्स 4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S–बॉक्स 5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S–बॉक्स 6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S–बॉक्स 7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S–बॉक्स 8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

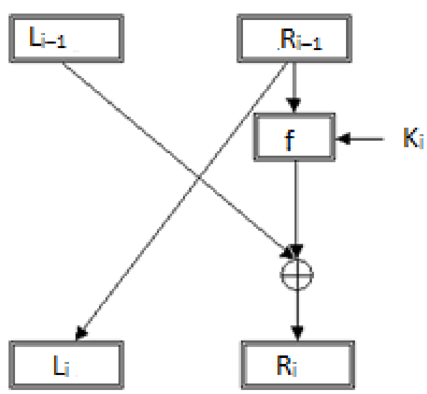
सरलीकृत DES:

सरलीकृत DES एक एल्गोरिथम (कलनविधि) है जो DES की कई विशेषताओं को रखता है, लेकिन DES की तुलना में बहुत आसान है। DES के समान, यह एल्गोरिथम (कलनविधि) भी एक ब्लॉक सिफर (खण्ड कूटलेख) है।

ब्लॉक आकारः सरलीकृत DES में, 12 बिट्स के ब्लॉक पर एन्क्रिप्शन/डिक्रिप्शन किया जाता है। प्लेन–टेक्स्ट/सिफर–टेक्स्ट को 12 बिट्स के ब्लॉक में बांटा जाता है और प्रत्येक ब्लॉक पर एल्गोरिथम (कलनविधि) लागू होता है।

कुंजीः कुंजी में 9 बिट्स होते हैं। एन्क्रिप्शन के iवें चक्र के लिए कुंजी K_i, K के 8 बिट्स का उपयोग करके प्राप्त की जाती है, जिसका आरंभ iवें बिट से होता है। उदाहरण के लिए यदि K = 111000111, तब $K_1 = 11100011$, $K_3 = 10001111$ और $K_{10} = K_1 = 11100011$.

एल्गोरिथम (कलनविधि)**:** 12 बिट्स का ब्लॉक L_0R_0 के रूप में लिखा जाता है, जहाँ L_0 में पहले 6 बिट्स और R_0 में अंतिम 6 बिट होते हैं। एल्गोरिथम (कलनविधि) का iवां चक्र K से व्युत्पन्न 8–बिट K_i का प्रयोग कर आउटपुट L_iR_i को इनपुट $L_{i-1}R_{i-1}$ स्थानान्तरित करता है।



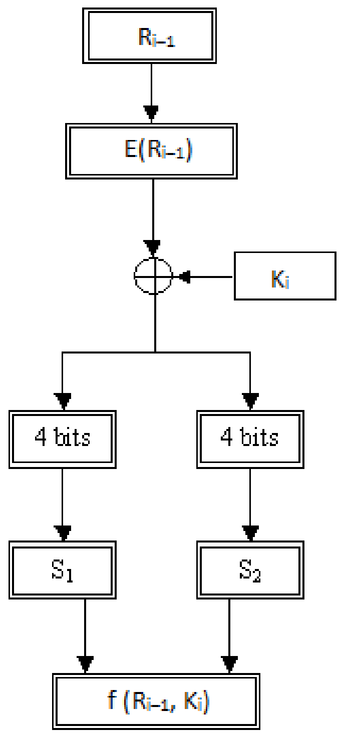
(चित्र क्र0 3.5; स्त्रोतः इंटरनेट से साभार)

iवें चक्र के लिए आउटपुट निम्न प्रकार प्राप्त किया जाता हैः

$L_i = R_{i-1}$ और $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

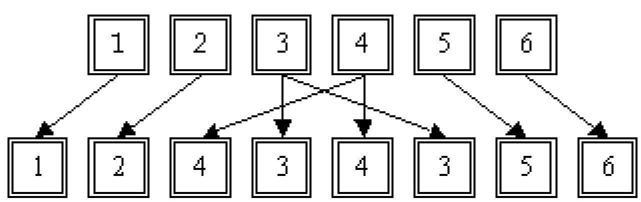
यह संक्रिया चक्र की एक निश्चित संख्या के लिए किया जाता है, माना n, और L_nR_n का उत्पादन करता है। सिफर–टेक्स्ट L_nR_n होगा। एन्क्रिप्शन और डिक्रिप्शन एक ही विधि से किया जाता है अतिरिक्त इसके कि कुंजियों को व्युत्क्रम क्रम में चुना जाता है। एन्क्रिप्शन के लिए कुंजी $K_1, K_2 \ldots\ldots K_n$ होगी और डिक्रिप्शन के लिए कुंजी $K_n, K_{n-1} \ldots\ldots K_1$ होगी।

फलन **$f(R_{i-1},K_i)$:** नीचे दिए गए चित्र में चित्रित फलन $f(R_{i-1},K_i)$, को निम्नलिखित चरणों में वर्णित किया गया है।



(चित्र क्र0 3.6; स्त्रोतः इंटरनेट से साभार)

1. निम्नलिखित विस्तार फलन का उपयोग करके 6–बिट का विस्तार किया जाता है। विस्तार फलन 6–बिट का इनपुट लेता है और 8–बिट का आउटपुट उत्पन्न करता है। यह आउटपुट दो S–बॉक्स के लिए इनपुट है



विस्तार फलन $E(R_{i-1})$

(चित्र क्र0 3.7)

2. पिछले चरण से प्राप्त 8–बिट आउटपुट कुंजी K_i के साथ XOR है।
3. 8–बिट आउटपुट दो ब्लॉक में बांटा जाता है। पहले ब्लॉक में पहले 4 बिट्स होते हैं और अंतिम चार बिट्स दूसरे ब्लॉक को बनाते हैं। पहला ब्लॉक पहले S–बॉक्स S_1 के लिए इनपुट है और दूसरा ब्लॉक दूसरे S–बॉक्स S_2 के लिए इनपुट है।
4. S–बॉक्स इनपुट के रूप में 4 बिट लेते हैं और आउटपुट के रूप में 3 बिट का उत्पादन करते हैं। इनपुट का पहला बिट S–बॉक्स से पंक्ति का चयन करने के लिए उपयोग में लाया जाता है, पहली पंक्ति के लिए 0 और दूसरी पंक्ति के लिए 1। स्तम्भ का चयन करने के लिए अंतिम 3 बिट्स का उपयोग किया जाता है।

उदाहरण के लिए, माना विस्तार फलन से आउटपुट 11010010 प्राप्त होता है, तो 1101 S_1 बॉक्स के लिए इनपुट होगा और 0010 S_2 बॉक्स के लिए इनपुट होगा। S_1 बॉक्स का आउटपुट 111 होगा, इनपुट का पहला बिट 1 है इसलिए दूसरी पंक्ति का चयन करें और 101 6वें स्तम्भ का चयन करेगा। इसी प्रकार S_2 बॉक्स से आउटपुट 110 प्राप्त होगा।

5. S–बॉक्स से प्राप्त आउटपुट को 6 बिट्स के एक ब्लॉक के साथ संयोजित किया जाता है। ये 6 बिट्स फलन $f(R_{i-1}, K_i)$ का आउटपुट होंगे। उपरोक्त उदाहरण में हमारे पास S_1 आउटपुट 111 और S_2 आउटपुट 110 है। इसलिए फलन $f(R_{i-1}, K_i)$ के लिए आउटपुट 111110 होगा, S_1 आउटपुट S_2 आउटपुट का अनुसरण करेगा।

S_1 और S_2 बॉक्स नीचे दिखाए गए हैं।

S1-बॉक्स

101	010	001	110	011	100	111	000
001	100	110	010	000	111	101	011

S2-बॉक्स

100	000	110	101	111	001	011	010
101	011	000	111	110	010	001	100

उदाहरणः

निम्न उदाहरण दो चक्रों की व्याख्या करता है। माना इनपुट संदेश 100010110101 है और कुंजी 111000111 है।

एन्क्रिप्शनः

चक्र 1 (i = 0)

1. $L_0 = 100010$ और $R_0 = 110101$; $K_1 = 11100011$.
2. $E(R_0) = 11101001$.
3. $E(R_0) \oplus K_1 = 11101001 \oplus 11100011 = 00001010$.
4. $S_1(0000) = 101$, $S_2(1010) = 000$, $\rightarrow f(R_0, K_1) = 101000$
5. $f(R_0, K_1) \oplus L_0 = 101000 \oplus 100010 = 001010$.
6. अब सूत्र $L_i = R_{i-1}$ और $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ का प्रयोग करें, हमें प्राप्त होता है,
   $L_1 = 110101$ और $R_1 = 001010$.

चक्र 2 (i = 1)

1. $L_1 = 110101$ और $R_1 = 001010$; $K_2 = 11000111$.
2. $E(R_1) = 00010110$.
3. $E(R_1) \oplus K_1 = 00010110 \oplus 11000111 = 11010001$.
4. $S_1(1101) = 111$; $S_2(0001) = 000$; $\rightarrow f(R_1, K_2) = 111000$
5. $f(R_1, K_2) \oplus L_1 = 111000 \oplus 110101 = 001101$.
6. अब सूत्र $L_i = R_{i-1}$ और $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ का प्रयोग करें, हमें प्राप्त होता है,
   $L_2 = 001010$ और $R_2 = 001101$.

   अतः एन्क्रिप्ट संदेश $R_2 L_2 = 001101001010$ है।

डिक्रिप्शनः

चक्र 1 (i = 0)

1. $L_0 = 001101$ और $R_0 = 001010$; $K_2 = 11000111$.
2. $E(R_0) = 00010110$.
3. $E(R_0) \oplus K_1 = 00010110 \oplus 11000101 = 11010001$.

4. $S_1(1101) = 121$; $S_2(0001) = 000$; $\rightarrow f(R_0, K_2) = 111000$
5. $f(R_0, K_2) \oplus L_0 = 111000 \oplus 001101 = 110101$.
6. अब सूत्र $L_i = R_{i-1}$ और $R_i = L_{i-1} \oplus f(R_{i-1}, K_{n-i})$ का प्रयोग करें, हमें प्राप्त होता है,
   $L_1 = 001010$ और $R_1 = 111000$.

चक्र 2 (i = 1)

1. $L_1 = 001010$ और $R_1 = 111000$; $K_1 = 11100011$.
2. $E(R_1) = 00010110$.
3. $E(R_1) \oplus K_1 = 11101001 \oplus 11100011 = 00001010$.
4. $S1(0000) = 101$; $S2(1010) = 000$; $\rightarrow f(R_1, K_1) = 101000$
5. $f(R_1, K_1) \oplus L_1 = 101000 \oplus 001010 = 100010$.
6. अब सूत्र $L_i = R_{i-1}$ और $R_i = L_{i-1} \oplus f(R_{i-1}, K_{n-i})$ का प्रयोग करें, हमें प्राप्त होता है,
   $L_2 = 110101$ और $R_2 = 100010$.

अतः डिक्रिप्ट (अकूटित) संदेश $R_2 L_2 = 100010110101$ है, जोकि मूल प्लेन–टेक्स्ट (साधारण–पाठ) संदेश है।

3.3 एडवांस्ड एन्क्रिप्शन स्टैंडर्ड (उन्नत कूटित मानक):

अधिक लोकप्रिय और व्यापक रूप से अपनाया जाने वाला सममित एन्क्रिप्शन एल्गोरिथम (कलनविधि) उन्नत एन्क्रिप्शन (कूटित) मानक (AES) है। यह ट्रिपल (triple) DES की तुलना में कम से कम छह गुना तेज पाया जाता है।

DES के लिए एक प्रतिस्थापन की आवश्यकता थी क्योंकि इसके कुंजी का आकार बहुत छोटा था। बढ़ती कम्प्यूटिंग शक्ति के साथ, इसे संपूर्ण कुंजी खोज कर आक्रमण करने के विरूद्ध माना जाता था। त्रिक DES को इस कमी को दूर करने के लिए अभिकल्पित किया गया था लेकिन यह धीमा पाया गया था।

AES की विशेषतायें निम्न हैं:

- सममित कुंजी सममित ब्लॉक सिफर (खण्ड कूटलेख)
- 128–बिट डेटा, 128/192/256–बिट कुंजी
- ट्रिपल DES से शक्तिशाली और तेज
- पूर्ण विनिर्देश और डिजाइन विवरण प्रदान करता है
- सी और जावा में लागू सॉफ्टवेयर

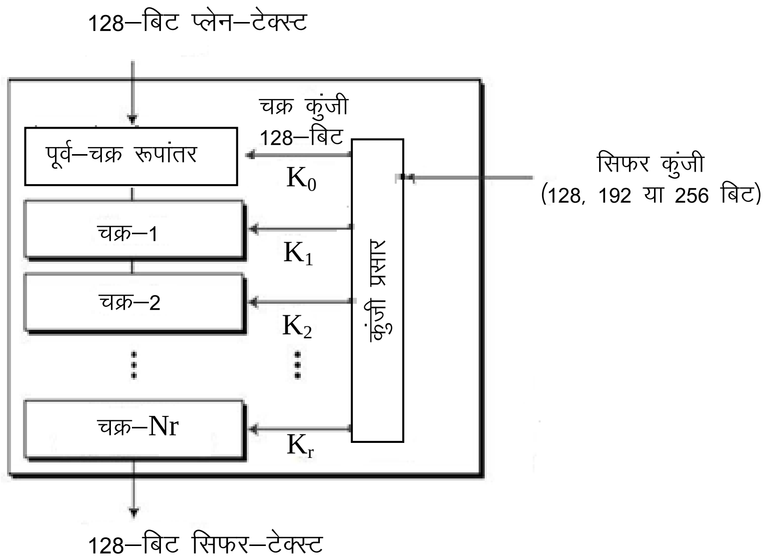
AES पर संक्रियायें:

AES फीस्टल सिफर के स्थान पर एक पुनरावृत्ति है। यह 'प्रतिस्थापन–क्रमपरिवर्तन नेटवर्क' पर आधारित है। इसमें लिंक्ड ऑपरेशंस की एक श्रृंखला शामिल है, जिनमें से कुछ विशिष्ट आउटपुट (प्रतिस्थापन) द्वारा इनपुट को प्रतिस्थापित करने में शामिल हैं और अन्य बिट्स का क्रमपरिवर्तन करने में शामिल हैं।

AES बिट्स के स्थान पर अपनी सभी गणना बाइट्स पर करता है। इसलिए, AES एक प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक के 128 बिट्स को 16 बाइट्स के रूप में मानता है। इन 16 बाइट्स को चार स्तंभों और चार पंक्तियों में व्यवस्थित करने के लिए आव्यूह के रूप में व्यवस्थित किया जाता है।

DES के विपरीत, AES में चक्रों की संख्या परिवर्तनीय है और कुंजी की लंबाई पर निर्भर करती है। AES 128–बिट कुंजियों के लिए 10 चक्र, 192–बिट कुंजियों के लिए 12 चक्र और 256–बिट कुंजियों के लिए 14 चक्रों का उपयोग करता है। इनमें से प्रत्येक चक्र एक अलग 128–बिट चक्र कुंजी का उपयोग करता है, जिसे मूल AES कुंजी से गणना की जाती है।

AES की संरचना निम्न चित्र में दी गई है –



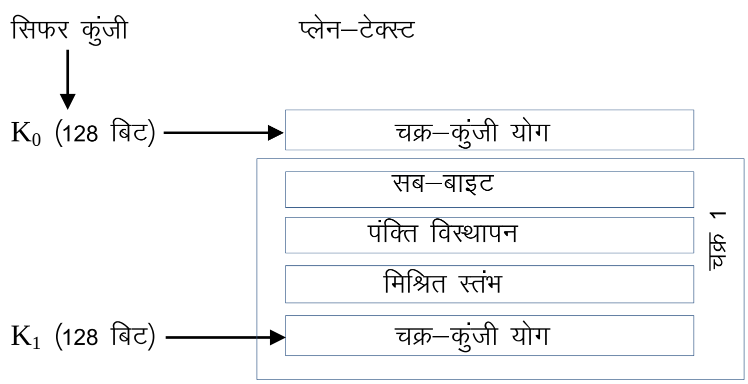
(चित्र क्र0 3.8)

चक्रों (R) की संख्या और सिफर कुंजी आकार के मध्य संबंधः

R	**कुंजी आकार**
10	128
12	192
14	256

एन्क्रिप्शन विधिः

यहाँ, हम AES एन्क्रिप्शन के एक विशिष्ट चक्र के विवरण तक सीमित हैं। प्रत्येक चक्र में चार उप–प्रक्रियाएं होती हैं। प्रथम चक्र की प्रक्रिया को नीचे दर्शाया गया है –



बाइट प्रतिस्थापनः

योजना में दिए गए एक निश्चित तालिका (S–बॉक्स) को देखकर 16 इनपुट बाइट प्रतिस्थापित किए जाते हैं। परिणाम चार पंक्तियों और चार स्तंभों के एक आव्यूह के रूप में होता है।

पंक्ति स्थानान्तरणः

आव्यूह की चार पंक्तियों में से प्रत्येक बाईं ओर स्थानांतरित हो जाती है। कोई भी प्रविष्टि जो अलग होती है, पंक्ति के दाईं ओर पुनः प्रविष्ट की जाती है। स्थानान्तरण निम्नानुसार किया जाता हैः

- पहली पंक्ति को स्थानांतरित नहीं किया जाता है।
- दूसरी पंक्ति को बाईं ओर एक (बाइट) स्थिति पर स्थानांतरित किया जाता है।
- तीसरी पंक्ति को दो स्थिति बाईं ओर स्थानांतरित किया जाता है।
- चौथी पंक्ति को तीन स्थिति बाईं ओर स्थानांतरित किया जाता है।
- परिणाम एक नया आव्यूह प्राप्त होता है जिसमें समान 16 बाइट शामिल हैं लेकिन एक–दूसरे के संबंध में स्थानांतरित हो गए हैं।

मिश्रित स्तम्भः

चार बाइट्स के प्रत्येक स्तम्भ को अब विशेष गणितीय फलन का उपयोग करके परिवर्तित किया जाता है। यह फलन एक स्तम्भ के चार बाइट इनपुट (निवेश) के रूप में लेता है और मूल स्तम्भ को प्रतिस्थापित करने वाले चार पूरी तरह से नए बाइट आउटपुट के रूप में देता है। परिणामतः एक नया आव्यूह प्राप्त होता है जिसमें 16 नए बाइट शामिल हैं। स्मरण रहे कि यह प्रक्रिया अंतिम चक्र में नहीं की जाती है।

चक्र कुंजी का योग करनाः

आव्यूह के 16 बाइट्स को अब 128 बिट्स के रूप में माना जाता है और चक्र कुंजी के 128 बिट्स पर XOR संक्रिया की जाती है। यदि यह अंतिम चक्र है तो आउटपुट सिफर–टेक्स्ट (कूटलेख–पाठ) के रूप में प्राप्त होगा, अन्यथा, परिणामी 128 बिट्स को 16 बाइट्स के रूप में लेकर हम एक और चक्र आरंभ करते हैं।

डिक्रिप्शन प्रक्रियाः

AES सिफर–टेक्स्ट (कूटलेख–पाठ) के डिक्रिप्शन की प्रक्रिया एन्क्रिप्शन प्रक्रिया के समान है लेकिन विपरीत क्रम में होती है। प्रत्येक चक्र में विपरीत क्रम में आयोजित निम्न चार प्रक्रियाओं का समावेश होता हैः

- चक्र कुंजी का योग करना
- स्तम्भ को मिश्रित करना
- पंक्तियों को स्थानान्तरित करना
- बाइट का प्रतिस्थापन करना

चूंकि प्रत्येक चक्र में उप–प्रक्रिया विपरीत विधि से होती है, इसलिए फीस्टल सिफर के विपरीत, एन्क्रिप्शन और डिक्रिप्शन एल्गोरिथम (कलनविधि) को पृथक से लागू करने की आवश्यकता होती है।

AES विश्लेषणः

वर्तमान में क्रिप्टोग्राफी (कूटलेखन) में, AES व्यापक रूप से अपनाया जाता है तथा हार्डवेयर और सॉफ्टवेयर दोनों में समर्थित है। आज तक, AES के विरूद्व कोई व्यावहारिक क्रिप्टैनालिटिक (कूटवैश्लेषिक) आक्रमणों की खोज नहीं हुई है। इसके अतिरिक्त, AES ने मुख्य लंबाई की लचीलापन निर्मित की है, जो संपूर्ण कुंजी खोज करने की क्षमता में प्रगति के विरूद्व 'भावी–प्रमाणन' की एक डिग्री की अनुमति देता है।

हालांकि, DES के लिए, AES सुरक्षा केवल तभी आश्वस्त होती है जब इसे सही विधि से कार्यान्वित किया जाता है और अच्छे कुंजी प्रबंधन को नियोजित किया जाता है।

3.4 इन्टरनेशनल डाटा एन्क्रिप्शन एल्गोरिथम (अंतर्राष्ट्रीय आंकड़ा कूटित कलन विधि):

IDEA एक अन्य ब्लॉक सिफर (खण्ड कूटलेख) एल्गोरिथम (कलनविधि) के विपरीत है, जिसका असॉम की स्विस फर्म द्वारा पेटेंट किया गया है। IDEA को लोकप्रिय एन्क्रिप्शन प्रोग्राम पीजीपी के अंदर उपयोग किए जाने वाले ब्लॉक सिफर (खण्ड कूटलेख) एल्गोरिथम (कलनविधि) के रूप में जाना जाता है।

IDEA एल्गोरिथम (कलनविधि) में कुछ चरण शामिल हैं, आरंभ में ऐसा आभास होता है कि यह एक ब्लॉक सिफर (खण्ड कूटलेख) के स्थान पर एक अव्युत्क्रमणीय हैश फंक्शन (द्रुतान्वेषण फलन) हो सकता है। साथ ही, यह किसी भी तालिका या S–बॉक्स के उपयोग से बचाता है।

IDEA 52 उपकुंजियों का उपयोग करता है, प्रत्येक 16 बिट लंबा होता है। प्रत्येक चक्र के समय दो बिट का उपयोग उचित होता है, और चार बिट का प्रयोग प्रत्येक चक्र के पूर्व और अंतिम चक्र के उपरान्त किया जाता है। इसमें आठ चक्र होते हैं।

IDEA में प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक चार चतुर्थांशों में बांटा गया है, प्रत्येक 16 बिट लंबा है। 16 बिट परिणाम जनित करने के लिए दो 16 बिट मानों को संयोजित करने हेतु आईडीईए में तीन संक्रियाओं का उपयोग किया जाता है। योग, XOR और गुणा। योग एक सामान्य अंकगणितीय योग के समान होता है, लेकिन हासिल के साथ। मॉड्यूल 65,536। IDEA में उपयोग किया जाने वाला गुणा को कुछ स्पष्टीकरण की आवश्यकता होती है।

शून्य द्वारा गुणा हमेशा शून्य उत्पन्न करता है, और व्युत्क्रमणीय नहीं है। गुणा मॉड्यूलो n भी व्युत्क्रमणीय नहीं है, जब भी यह उस संख्या से होता है जो n के सापेक्षतः अभाज्य है। IDEA में गुणा का उपयोग किये जाने के लिए यह आवश्यक है कि यह सदैव व्युत्क्रमणीय हो। यह गुणा आईडीईए शैली के लिए सत्य है।

संख्या 65537, जो $2^{16} + 1$ है, एक अभाज्य संख्या है। (संयोग से, $2^8 + 1$ या 257 भी अभाज्य है, और $2^4 + 1$ या 17 भी है, लेकिन $2^{32} + 1$ अभाज्य नहीं है, इसलिए IDEA का 128–बिट ब्लॉक आकार तक तुच्छ रूप से माप नहीं किया जा सकता है।) इस प्रकार, यदि कोई 1 से 65536 तक संख्याओं के लिए लैटिन वर्ग बनाकर एक गुणा तालिका बनाता है, तो प्रत्येक पंक्ति और स्तम्भ में केवल एक बार प्रत्येक संख्या होगी, और एक व्युत्क्रमणीय संक्रिया प्रदान करेगा। वह संख्या जिसे 16 बिट्स सामान्यतः प्रदर्शित करता है 0 से 65535 के मध्य (या शायद अधिक सामान्यतः –32,768 से 32,767 तक) हैं।

IDEA में, गुणा के प्रयोजनों के लिए, सभी शून्य रखने वाले 16 बिट शब्द को 65536 संख्या का प्रतिनिधित्व करने के लिए माना जाता है। अन्य संख्याओं को पारंपरिक अहस्ताक्षरित अंकन (notation) में दर्शाया जाता है, और गुणा मॉड्यूलो अभाज्य संख्या 65,537 है।

IDEA का विवरण:

माना प्लेन–टेक्स्ट (साधारण–पाठ) के चार चतुर्थांश A, B, C और D हैं, और K(1) से K(52) तक 52 उपकुंजियाँ हैं। प्रथम चक्र के पूर्व निम्न कार्य करें:

- A को K(1) से गुणा करें।
- B में K(2) का योग करें।
- C में K(3) का योग करें।
- D को K(4) से गुणा करें।

प्रथम चक्र में निम्न शामिल हैं:

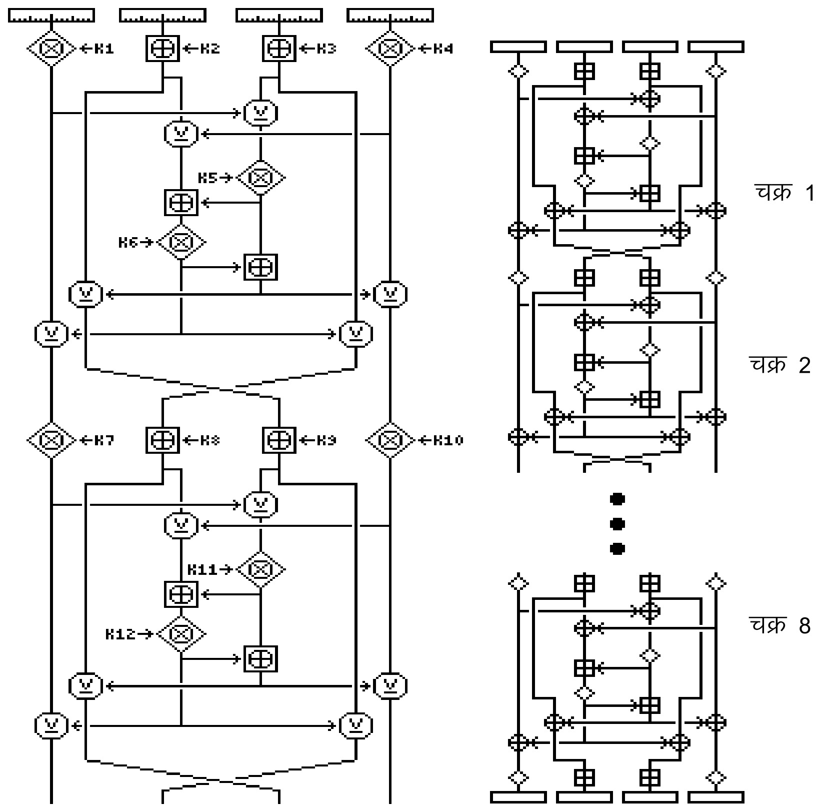
- A XOR C की गणना करें (माना यह E है)।
- B XOR D की गणना करें (माना यह F है)।
- E को K(5) से गुणा करें। E के नवीन मान को F से योग करें।
- F के नवीन मान को K(6) द्वारा गुणा करें। परिणाम को E से योग करें, जो F का नया मान भी है।

A और C दोनों के साथ F के वर्तमान मान को XOR द्वारा संक्रिया कर A और C को परिवर्तित करें। इसीप्रकार B और D दोनों के साथ E के वर्तमान मान को XOR द्वारा संक्रिया कर B और D को परिवर्तित करें। B और C का आपस में विनिमय करें।

इन सभी की पुनरावृत्ति आठ बार करें। द्वितीय बार K(7) से K(12) का उपयोग करें। आठवीं बार K(43) से K(48) का उपयोग करें। स्मरण रहे B और C का आपस में विनिमय 8वें चक्र के उपरान्त नहीं किया जाता है। तब

- A को K(49) से गुणा करें।
- B में K(50) का योग करें।
- C में K(51) का योग करें।
- D को K(52) से गुणा करें।

निम्नलिखित चित्रों का परीक्षण करके IDEA एन्क्रिप्शन की जटिलताओं को कुछ हद तक स्पष्ट किया जा सकता है:



(चित्र क्र0 3.9; स्त्रोतः इंटरनेट से साभार)

डिक्रिप्शनः

IDEA में डिक्रिप्शन की विधि एन्क्रिप्शन विधि के व्युत्क्रम होती है। जिसे निम्न प्रकार स्पष्ट किया गया है:

डिक्रिप्शन के लिए प्रथम चार कुंजी निम्न हैं:

KD(1) = 1/K(49)
KD(2) = – K(50)
KD(3) = – K(51)
KD(4) = 1/K(52)

और वे उसी उपरोक्त स्वरूप का पालन नहीं करते हैं जो शेष उपकुंजियों का पालन करता है।

निम्नलिखित की आठ बार पुनरावृत्ति की जाती है, प्रत्येक डिक्रिप्शन कुंजी की अनुक्रमणिका में 6 का योग करते हैं और प्रत्येक एन्क्रिप्शन कुंजी की अनुक्रमणिका से 6 को घटाया जाता है:

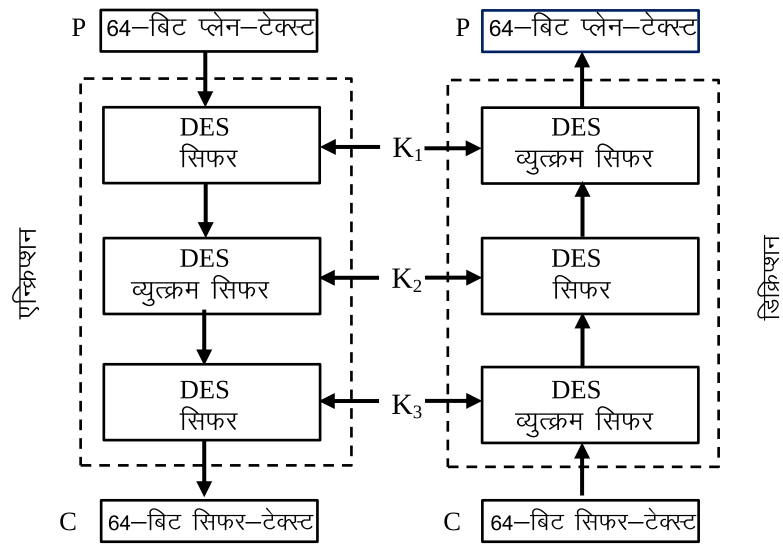
KD(5) = K(47)
KD(6) = K(48)
KD(7) = 1/K(43)
KD(8) = – K(45)
KD(9) = – K(44)
KD(10) = 1/K(46)

उपकुंजी का जननः

IDEA की 128–बिट कुंजी को प्रथम आठ उपकुंजी K(1) से K(8) के रूप में लिया जाता है। 25–बिट के बायीं ओर स्थानान्तरित होने के उपरान्त आगामी आठ उपकुंजियां उसी पूर्व प्रक्रिया के समान प्राप्त की जाती हैं, और इसकी पुनरावृत्ति तब तक की जाती है जब तक सभी एन्क्रिप्शन उपकुंजियां प्राप्त नहीं होतीं।

उपकुंजी जनन की यह विधि नियमित है, और यह एक कमजोरी हो सकती है। हालांकि, IDEA को अत्यधिक सुरक्षित माना जाता है, जो अब तक शैक्षिक समुदाय द्वारा किए गए आक्रमण के उपरान्त भी स्थिर है।

3.5 त्रिक DES:



(चित्र क्र0 3.10)

1990 के उपरान्त DES के विरूद्व संपूर्ण कुंजी खोजों की गति ने DES के उपयोगकर्ताओं के बीच असुविधा उत्पन्न की। हालांकि, उपयोगकर्ता DES को प्रतिस्थापित नहीं करना चाहते थे क्योंकि बड़े सुरक्षा आर्किटेक्चर (वास्तुकला) में व्यापक रूप से अपनाए गए और एम्बेडेड एन्क्रिप्शन एल्गोरिथम (कलनविधि) को प्रतिस्थापित करने के लिए इसमें बहुत समय और पैसा लगता है। व्यावहारिक दृष्टिकोण DES को पूरी तरह से त्यागना नहीं था, लेकिन जिस प्रकार से DES का उपयोग किया जाता है उस प्रक्रिया में परिवर्तन करना था। इससे त्रिक DES की संशोधित योजना प्राप्त हुई।

DES में अल्प परिवर्तन करके त्रिक DES को निर्मित किया गया है। हालांकि, DES की तुलना में यह तीन गुना मंद गति वाला है, अगर इसे उचित रूप से उपयोग किया जाता है, तो यह अधिक सुरक्षित हो सकता है। आज के परिदृश्य में, त्रिक DES, DES की तुलना में अधिक व्यापक रूप से लागू किया गया है। ऐसा इसलिए है क्योंकि DES को उन्नत तकनीक की मदद से खंडित करना आसान है, जो आज व्यापक रूप से उपलब्ध है। त्रिक DES में उपयोग की जाने वाली लंबी कुंजी की लंबाई के कारण त्रिक DES एक बेहद विश्वसनीय समाधान साबित हुआ है। कुंजी की यह विस्तारित लंबाई क्षुद्र आक्रमणों को समाप्त करने में एक महत्वपूर्ण भूमिका निभाती है।

हम EDE (Encrypt, Decrypt, Encrypt) प्रक्रिया के माध्यम से त्रिक पास DES का उपयोग कर अपने क्रिप्टोग्राफिक (कूटलेखीय) प्रणाली की प्रभावी कुंजी की लंबाई बढ़ा सकते हैं। जब हम त्रिक पास DES का उपयोग करते हैं, तो यह पहले प्लेन–टेक्स्ट (साधारण–पाठ) डेटा को 56–बिट कुंजी के साथ एन्क्रिप्ट (कूटित) करता है। इसलिए प्राप्त किए गए सिफर–टेक्स्ट (कूटलेख–पाठ) को एक अलग कुंजी का उपयोग करके डिक्रिप्ट किया जाता है।

जब हम कुछ पृथक कुंजी के साथ सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट (अकूटित) करते हैं तो यह कुछ गारबेज देता है। अंत में, हम प्रथम कुंजी के साथ गारबेज एन्क्रिप्ट (कूटित) करते हैं। एन्क्रिप्शन, डिक्रिप्शन, और फिर एन्क्रिप्शन के लिए त्रिक पास DES का उपयोग करने की इस प्रक्रिया आमतौर पर EDE के रूप में जाना जाता है। चित्र क्र0 3.10 त्रिक DES की प्रक्रिया बताते हैं।

संयोग से, त्रिक DES के दो प्रकार हैं जिन्हें 3–कुंजी त्रिक DES (3TDES) और 2–कुंजी त्रिक DES (2TDES) कहा जाता है।

3–कुंजी त्रिक DES (3TDES):

3TDES का उपयोग करने के पूर्व, उपयोगकर्ता पहले एक 3TDES कुंजी K को जनित और वितरित करता है, जिसमें तीन पृथक–पृथक DES कुंजी K_1, K_2 और K_3 होते हैं। इसका अर्थ है कि वास्तविक 3TDES कुंजी की लंबाई $3 \times 56 = 168$ बिट्स है। एन्क्रिप्शन योजना को उपरोक्त चित्र में दिखाया गया है। एन्क्रिप्शन–डिक्रिप्शन प्रक्रिया निम्नानुसार हैः

- कुंजी K_1 के साथ एकल DES का उपयोग करके प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को एन्क्रिप्ट (कूटित) करें।
- अब कुंजी K_2 के साथ एकल DES का उपयोग करके चरण 1 के आउटपुट को डिक्रिप्ट (अकूटित) करें।
- अंत में, कुंजी K_3 के साथ एकल DES का उपयोग करके चरण 2 के आउटपुट को एन्क्रिप्ट (कूटित) करें।
- चरण 3 का आउटपुट सिफर–टेक्स्ट (कूटलेख–पाठ) है।
- एक सिफर–टेक्स्ट (कूटलेख–पाठ) का डिक्रिप्शन एक व्युत्क्रम प्रक्रिया है। उपयोगकर्ता पहले K_3 का उपयोग करके डिक्रिप्ट (अकूटित) करता है, फिर K_2 के साथ एन्क्रिप्ट (कूटित) करता है, और अंततः K_1 के साथ डिक्रिप्ट (अकूटित) करता है।

उपरोक्त रचना के कारण ट्रिपल DES एक एन्क्रिप्ट–डिक्रिप्ट–एन्क्रिप्ट प्रक्रिया है। K_1, K_2 और K_3 का एक ही मान व्यवस्थित करके एकल DES के लिए 3TDES कार्यान्वयन का उपयोग करना संभव है। यह DES के साथ पश्चवर्ती संगतता प्रदान करता है।

त्रिक DES का दूसरा संस्करण 2TDES, 3TDES के समान है, मात्र अन्तर यह है कि K_3 को K_1 द्वारा प्रतिस्थापित किया जाता है। दूसरे शब्दों में, उपयोगकर्ता कुंजी K_1 के साथ प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को एन्क्रिप्ट (कूटित) करता है, फिर कुंजी K_2 के साथ डिक्रिप्ट (अकूटित) करता है, और अंततः K_1 के साथ एन्क्रिप्ट (कूटित) करता है। अतः 2TDES, 112 बिट्स की लंबाई की एक कुंजी रखता है।

त्रिक DES सिस्टम एकल DES की तुलना में अधिक सुरक्षित है, लेकिन यह एकल DES का उपयोग करके एन्क्रिप्शन की तुलना में स्पष्ट रूप से मंद प्रक्रिया है।

अभ्यास

1. आधुनिक सममित कुंजी एन्क्रिप्शन (कूटित) को समझाइए।
2. ब्लॉक सिफर (खण्ड कूटलेख) क्या है?
3. स्ट्रीम सिफर (प्रवाह कूटलेख) से क्या समझते हैं?
4. डाटा एन्क्रिप्शन स्टैंडर्ड (आँकड़ा कूटित मानक) की अवधारणा को स्पष्ट करें।
5. एडवांस्ड एन्क्रिप्शन स्टैंडर्ड (उन्नत कूटित मानक) को विस्तार से समझाइए।
6. इन्टरनेशनल डाटा एन्क्रिप्शन एल्गोरिथम (अंतर्राष्ट्रीय आंकड़ा कूटित कलन विधि) से क्या समझते हैं?
7. त्रिक DES की अवधारणा को स्पष्ट करें।

अध्याय – 4

ऑपरेशन के ब्लॉक सिफर (खण्ड कूटलेख) मोड्स

इस अध्याय में, हम एक ब्लॉक सिफर (खण्ड कूटलेख) के संचालन के विभिन्न विधियों पर चर्चा करेंगे। ये एक व्यापक ब्लॉक सिफर (खण्ड कूटलेख) के लिए प्रक्रियात्मक नियम हैं। दिलचस्प बात यह है कि विभिन्न मोड्स पृथक–पृथक गुणों को प्राप्त करते हैं जो अंतर्निहित ब्लॉक सिफर (खण्ड कूटलेख) की सुरक्षा को जोड़ते हैं।

एक ब्लॉक सिफर (खण्ड कूटलेख) निश्चित आकार के डेटा ब्लॉक (आँकड़ा खण्ड) को संसाधित करता है। आमतौर पर, किसी संदेश का आकार ब्लॉक आकार से बड़ा होता है। इसलिए, लंबे संदेश को अनुक्रमिक संदेश ब्लॉक्स की एक श्रृंखला में विभाजित किया जाता है, और सिफर इन ब्लॉक्स को एक समय में संचालित करता है।

क्रिप्टोग्राफी (कूटलेखन) में, संक्रिया का एक ब्लॉक सिफर (खण्ड कूटलेख) मोड एक एल्गोरिथ्म (कलनविधि) है जो गोपनीयता या प्रामाणिकता जैसी सूचना सुरक्षा प्रदान करने के लिए ब्लॉक सिफर (खण्ड कूटलेख) का उपयोग करता है। अपने आप में एक ब्लॉक सिफर (खण्ड कूटलेख) केवल बिट्स के एक निश्चित लंबाई वाले समूह के सुरक्षित क्रिप्टोग्राफिक ट्रांसफॉर्मेशन (एन्क्रिप्शन या डिक्रिप्शन) के लिए उपयुक्त है, जिसे ब्लॉक कहा जाता है। संक्रिया की विधि यह बताता है कि एक सिफर (कूटलेख) के एकल ब्लॉक संक्रिया को बार–बार कैसे लागू किया जाए, ताकि वह ब्लॉक से बड़े डेटा की मात्रा को सुरक्षित रूप से बदल सके।

अधिकांश मोड में एक अद्वितीय बाइनरी अनुक्रम की आवश्यकता होती है, जिसे अक्सर प्रत्येक एन्क्रिप्शन ऑपरेशन के लिए आरंभीकरण सदिश (IV) कहा जाता है। IV को कुछ मोड के लिए गैर–पुनरावृत्ति वाला होना चाहिए और साथ ही यादृच्छिक भी। प्रारंभीकरण सदिश का उपयोग यह सुनिश्चित करने के लिए किया जाता है कि समान प्लेन–टेक्स्ट (साधारण–पाठ) को समान कुंजी के साथ स्वतंत्र रूप से कई बार एन्क्रिप्ट किया गया हो तब भी पृथक–पृथक सिफर–टेक्स्ट (कूटलेख–पाठ) का उत्पादन किया जाता है। ब्लॉक सिफर (खण्ड कूटलेख) एक से अधिक ब्लॉक आकार पर काम करने में सक्षम हो सकता है, लेकिन परिवर्तन के दौरान ब्लॉक आकार हमेशा तय होता है। ब्लॉक सिफर (खण्ड कूटलेख) मोड पूरे ब्लॉक पर काम करते हैं और इसके लिए आवश्यक है कि डेटा का अंतिम भाग एक पूर्ण ब्लॉक में पैडेड हो, यदि यह वर्तमान ब्लॉक आकार से छोटा हो, तो। हालांकि, ऐसे मोड हैं जिन्हें पैडिंग की आवश्यकता नहीं होती है क्योंकि वे प्रभावी रूप से एक स्ट्रीम सिफर (प्रवाह कूटलेख) के रूप में एक ब्लॉक सिफर (खण्ड कूटलेख) का उपयोग करते हैं।

ऐतिहासिक रूप से, एन्क्रिप्शन मोड में डेटा संशोधन के विभिन्न परिदृश्यों के तहत उनकी त्रुटि प्रसार गुणों के संबंध में बड़े पैमाने पर अध्ययन किया गया है। बाद में विकास ने अखंडता संरक्षण को एक पूरी तरह से अलग क्रिप्टोग्राफिक (कूटलेखीय) लक्ष्य के रूप में माना। ऑपरेशन के कुछ आधुनिक मोड एक कुशल तरीके से गोपनीयता और प्रामाणिकता को जोड़ते हैं, और प्रामाणिक एन्क्रिप्शन मोड के रूप में जाना जाता है।

टीपः

1. एक आरंभीकरण सदिश (IV) या आरंभिक चर बिट्स का एक ब्लॉक है जो एन्क्रिप्शन को यादृच्छिक करने के लिए कई मोड्स द्वारा उपयोग किया जाता है और इसलिए पृथक सिफर–टेक्स्ट (कूटलेख–पाठ) उत्पन्न करने के लिए समान प्लेन–टेक्स्ट (साधारण–पाठ) को कई बार एन्क्रिप्ट (कूटित) किया जाता है, एक धीमी पुनः–कुंजीयन प्रक्रिया के लिए बिना आवश्यकता के।

   एक प्रारंभिक सदिश में एक कुंजी की तुलना में विभिन्न सुरक्षा आवश्यकताएं होती हैं, इसलिए IV को आमतौर पर गुप्त रहने की आवश्यकता नहीं होती है। हालांकि, अधिकांश दशाओं में, यह महत्वपूर्ण है कि एक प्रारंभिक सदिश का उपयोग एक ही कुंजी के तहत कभी नहीं किया जाता है। CBC और CFB के लिए, IV का पुनः उपयोग करने से प्लेन–टेक्स्ट (साधारण–पाठ) के पहले ब्लॉक के बारे में कुछ जानकारी प्रकट होती है, और दो संदेशों द्वारा साझा किए गए किसी भी सामान्य उपसर्ग के बारे में। OFB और CTR के लिए, IV का पुनः उपयोग पूरी तरह से सुरक्षा को नष्ट कर देता है।

2. क्रिप्टोग्राफी (कूटलेखन) में, पैडिंग कई अलग–अलग प्रथाओं को संदर्भित करता है जिसमें एन्क्रिप्शन से पहले एक संदेश की आरंभ, मध्य या अंत में डेटा (आँकड़ा) जोड़ना शामिल है। एक ब्लॉक सिफर (खण्ड कूटलेख) एक निश्चित आकार की इकाइयों पर काम करता है (जिसे ब्लॉक आकार के रूप में जाना जाता है), लेकिन संदेश कई प्रकार की लंबाई में आते हैं।

कुछ मोड (अर्थात् ECB और CBC) की आवश्यकता है कि अंतिम ब्लॉक एन्क्रिप्शन से पहले पैडेड हो। कई पैडिंग योजनाएं उपलब्ध हैं। सबसे सरल यह है कि अपनी लंबाई को कई ब्लॉक आकार तक लाने के लिए प्लेन–टेक्स्ट (साधारण–पाठ) में शून्य बाइट्स (null bytes) को जोड़ना है। लेकिन इस बात का ध्यान रखा जाना चाहिए कि प्लेन–टेक्स्ट (साधारण–पाठ) की मूल लंबाई फिर से प्राप्त की जा सके। उदाहरण के लिए, अगर प्लेन–टेक्स्ट (साधारण–पाठ) एक C भाषा के समान एक स्ट्रिंग है, जिसमें अंत में छोड़कर कोई शून्य बाइट्स नहीं है। थोड़ा अधिक जटिल मूल DES विधि है, जो एक एकल बिट को जोड़ने के लिए है, इसके बाद ब्लॉक को भरने के लिए पर्याप्त शून्य बिट्स; यदि संदेश एक ब्लॉक सीमा पर समाप्त होता है, तो एक पूरा पेडिंग ब्लॉक जोड़ा जाएगा।

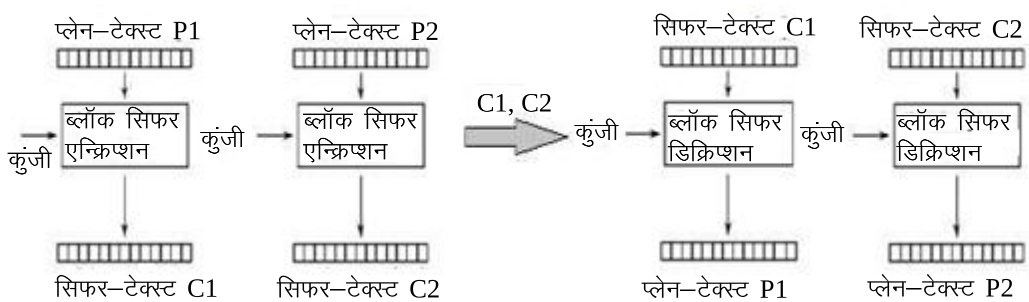
संक्रिया की कई विधियाँ परिभाषित हैं। इनमें से कुछ नीचे वर्णित हैं। सिफर (कूटलेख) मोड्स का उद्देश्य एनक्रिप्टेड डेटा (कूटित आँकड़ा) में उपलब्ध मास्क पैटर्न है, जो ECB की कमजोरी के वर्णन में वर्णित है।

4.1 इलेक्ट्रॉनिक कोड बुक मोड (ECB):

यह मोड क्रमिक रूप से सूचीबद्ध संदेश ब्लॉक की एक श्रृंखला को संसाधित करने का सबसे सीधा तरीका है।

संक्रियाः उपयोगकर्ता प्लेन–टेक्स्ट (साधारण–पाठ) का पहला ब्लॉक लेता है और इसे सिफर–टेक्स्ट (कूटलेख–पाठ) के पहले ब्लॉक का निर्माण करने के लिए कुंजी के साथ एन्क्रिप्ट (कूटित) करता है। फिर वह प्लेन–टेक्स्ट (साधारण–पाठ) का दूसरा ब्लॉक लेता है और उसी प्रक्रिया का अनुसरण करता है।

ECB मोड निर्धारक है, अर्थात, यदि प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक P1, P2,..., Pm को एक ही कुंजी के तहत दो बार एन्क्रिप्ट (कूटित) किया गया है, तो आउटपुट सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक समान होंगे। वास्तव में, किसी दिए गए कुंजी के लिए तकनीकी रूप से हम सभी संभावित प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक के लिए सिफर–टेक्स्ट (कूटलेख–पाठ) की एक कोडबुक बना सकते हैं। एन्क्रिप्शन तब केवल आवश्यक प्लेन–टेक्स्ट (साधारण–पाठ) की तलाश में प्रवेश करेगा और संबंधित सिफर–टेक्स्ट (कूटलेख–पाठ) का चयन करेगा। इस प्रकार, संक्रिया एक कोडबुक में कोड शब्दों के अभिहस्तांकन के अनुरूप है, और इसलिए एक आधिकारिक नाम मिलता है – संक्रिया का इलेक्ट्रॉनिक कोडबुक मोड (ECB)। इसका वर्णन इस प्रकार है –



(चित्र क्र0 4.1)

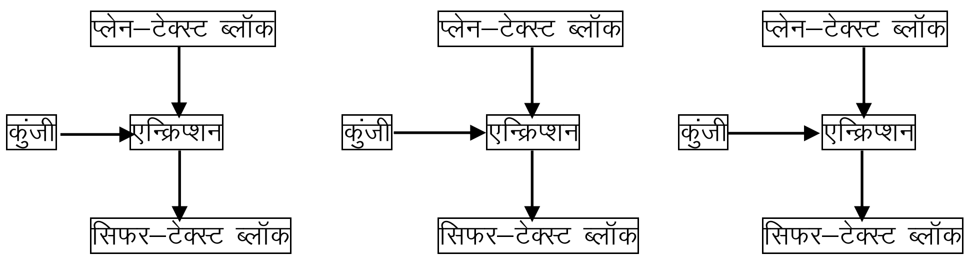
ECB मोड का विशलेषणः

वास्तव में, किसी भी अनुप्रयोगिक डेटा में आमतौर पर आंशिक जानकारी होती है जिसका अनुमान लगाया जा सकता है। उदाहरण के लिए, वेतन की सीमा का अनुमान लगाया जा सकता है।

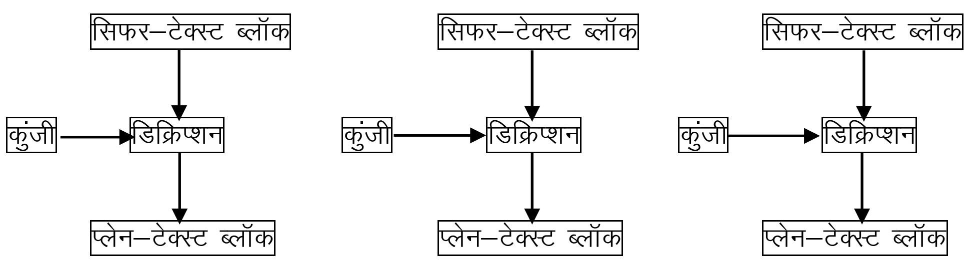
ECB से एक सिफर–टेक्स्ट (कूटलेख–पाठ) एक हमलावर को ट्रायल–एंड–एरर द्वारा प्लेन–टेक्स्ट (साधारण–पाठ) का अनुमान लगाने की अनुमति दे सकता है यदि प्लेन–टेक्स्ट (साधारण–पाठ) संदेश पूर्वकथनीय हो।

उदाहरण के लिए, यदि ECB मोड से एक सिफर–टेक्स्ट (कूटलेख–पाठ) को वेतन का आंकड़ा एन्क्रिप्ट (कूटित) करने के लिए जाना जाता है, तो थोड़ी संख्या में परीक्षण एक हमलावर को आंकड़ा पुनर्प्राप्त करने की अनुमति देगा। सामान्य तौर पर, हम एक नियतात्मक सिफर (कूटलेख) का उपयोग नहीं करना चाहते हैं, और इसलिए ECB मोड का उपयोग अधिकांश अनुप्रयोगों में नहीं किया जाना चाहिए।

एन्क्रिप्शन मोड का सबसे सरल मोड इलेक्ट्रॉनिक कोडबुक (ECB) मोड (पारंपरिक भौतिक कोडबुक के नाम पर) है। इसमें संदेश को ब्लॉक में विभाजित किया गया है, और प्रत्येक ब्लॉक को पृथक–पृथक एन्क्रिप्ट (कूटित) किया जाता है।



(चित्र क्र0 4.2: ECB मोड एन्क्रिप्शन)



(चित्र क्र0 4.3: ECB मोड डिक्रिप्शन)

इस पद्धति का नुकसान विसरण की कमी है। क्योंकि ECB समरूप प्लेन–टेक्स्ट ब्लॉक को समान सिफर–टेक्स्ट ब्लॉक में एन्क्रिप्ट करता है, यह डेटा प्रतिमान को अच्छी तरह से छिपा नहीं पाता है। कुछ अर्थों में, यह गंभीर संदेश गोपनीयता प्रदान नहीं करता है, और यह क्रिप्टोग्राफिक (कूटलेखीय) प्रोटोकॉल में उपयोग के लिए बिल्कुल भी अनुशंसित नहीं है।

ECB मोड को एक बिटमैप छवि को एन्क्रिप्ट (कूटित) करने के लिए उपयोग किया जाता है, जो समान रंग के बड़े क्षेत्रों का उपयोग करने के लिए ECB मोड में प्लेन–टेक्स्ट (साधारण–पाठ) आँकड़ा प्रतिमान छोड़ सकता है, जिसके लिए डिग्री का एक अच्छा उदाहरण देखा जा सकता है। हालांकि प्रत्येक व्यक्तिगत पिक्सेल का रंग एन्क्रिप्ट (कूटित) किया गया है, समग्र छवि अभी भी विच्छेदित हो सकती है, क्योंकि एन्क्रिप्टेड संस्करण में मूल रूप से पहचान किए गए रंगीन पिक्सेल का प्रतिमान रहता है।

ECB मोड भी अखंडता सुरक्षा के बिना प्रोटोकॉल बना सकता है और फिर से हमलों के लिए अतिसंवेदनशील होता है, क्योंकि प्रत्येक ब्लॉक बिल्कुल उसी तरह से डिक्रिप्ट (अकूटित) हो जाता है।

ECB का उपयोग करने के लाभः

- ➢ बिट्स के ब्लॉक का समानांतर एन्क्रिप्शन संभव है, इस प्रकार यह एन्क्रिप्शन की तीव्र विधि है।
- ➢ ब्लॉक सिफर (खण्ड कूटलेख) की सरल विधि है।

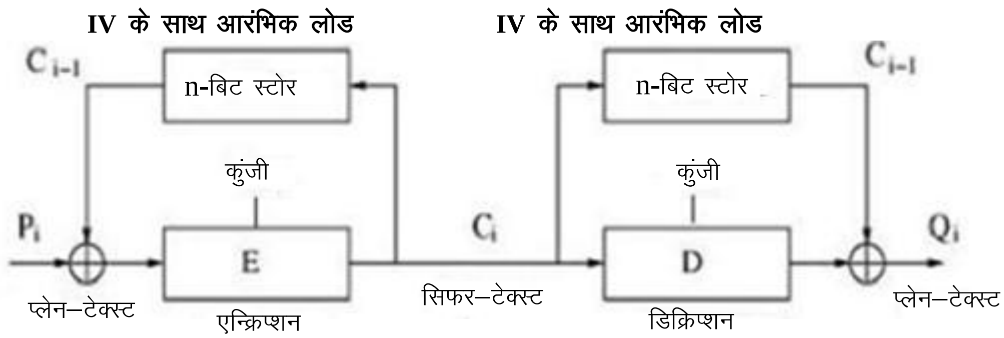
ECB का उपयोग करने के नुकसानः

- प्लेन–टेक्स्ट (साधारण–पाठ) और सिफर–टेक्स्ट (कूटलेख–पाठ) के मध्य सीधा संबंध होने से क्रिप्टोनालिसिस (कूटविश्लेषण) होने का खतरा है।

4.2 सिफर ब्लॉक (कूटलेख खण्ड) चेनिंग मोड (CBC):

संक्रिया का CBC मोड सिफर–टेक्स्ट (कूटलेख–पाठ) उत्पन्न करने के लिए संदेश पर निर्भरता प्रदान करता है और प्रणाली को गैर–नियतात्मक बनाता है।

संक्रियाः



(चित्र क्र0 4.4)

CBC मोड के संचालन को उपरोक्त चित्र में दर्शाया गया है। चरण इस प्रकार हैं –

- n–बिट आरंभीकरण सदिश (IV) को शीर्ष रजिस्टर में लोड करें।
- शीर्ष रजिस्टर में डेटा मान के साथ n–बिट प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को XOR करें।
- कुंजी K तथा अंतर्निहित ब्लॉक सिफर (खण्ड कूटलेख) के साथ XOR संक्रिया के परिणाम को एन्क्रिप्ट (कूटित) करें।
- शीर्ष रजिस्टर में सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को प्रविष्ट करें और तब तक संक्रिया जारी रखें जब तक सभी प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक संसाधित नहीं हो जाते।
- डिक्रिप्शन के लिए, IV डेटा को प्रथम सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक डिक्रिप्ट के साथ XOR किया जाता है। अगले सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को डिक्रिप्ट (अकूटित) करने के लिए प्रथम सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को IV के स्थान पर रजिस्टर में प्रविष्ट किया जाता है।

CBC मोड का विशलेषणः

CBC मोड में, वर्तमान प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को पिछले सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक में जोड़ा जाता है, और फिर परिणाम कुंजी के साथ एन्क्रिप्ट (कूटित) किया जाता है। डिक्रिप्शन इसी प्रकार व्युत्क्रम प्रक्रिया है, जिसमें वर्तमान सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट (अकूटित) करना और फिर परिणाम में पिछले सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को जोड़ना सम्मिलित है।

ECB पर CBC का लाभ यह है कि समान संदेश के लिए विभिन्न सिफर–टेक्स्ट (कूटलेख–पाठ) में IV परिणाम परिवर्तित होते हैं। ECB पर CBC का नुकसान यह है संचरण में त्रुटि को श्रृंखला प्रभाव के कारण डिक्रिप्शन के दौरान कुछ और ब्लॉक में प्रचारित किया जाता है।

यह उल्लेखनीय है कि CBC मोड एक प्रसिद्ध डेटा मूल प्रमाणीकरण तंत्र के लिए आधार बनाता है। इस प्रकार, यह उन अनुप्रयोगों के लिए एक लाभदायक है जहाँ सममित एन्क्रिप्शन और डेटा मूल प्रमाणीकरण दोनों की आवश्यकता होती है।

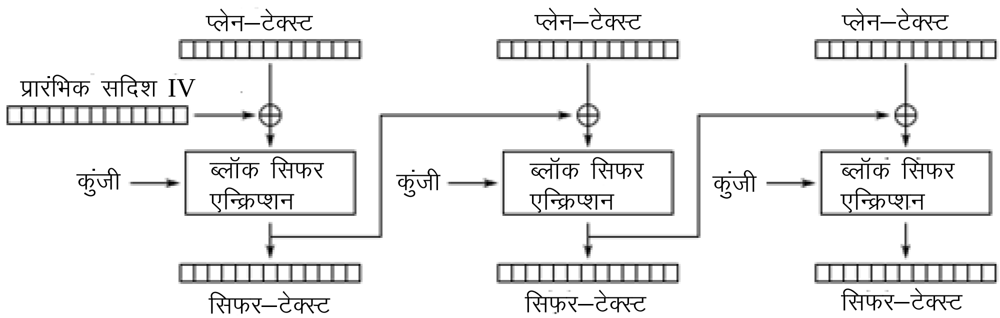
एहराम, मेयर, स्मिथ और तुचमैन ने 1976 में ऑपरेशन के सिफर ब्लॉक चेनिंग (CBC) मोड का आविष्कार किया। CBC मोड में, प्लेन–टेक्स्ट (साधारण–पाठ) का प्रत्येक ब्लॉक एन्क्रिप्टेड होने से पहले पूर्व सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक के साथ XORed होता है। इस प्रकार, प्रत्येक सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक उस बिंदु तक संसाधित सभी प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक पर निर्भर करता है। प्रत्येक संदेश को अद्वितीय बनाने के लिए, प्रथम ब्लॉक में एक आरंभीकरण सदिश का उपयोग किया जाना चाहिए।

CBC के लाभः

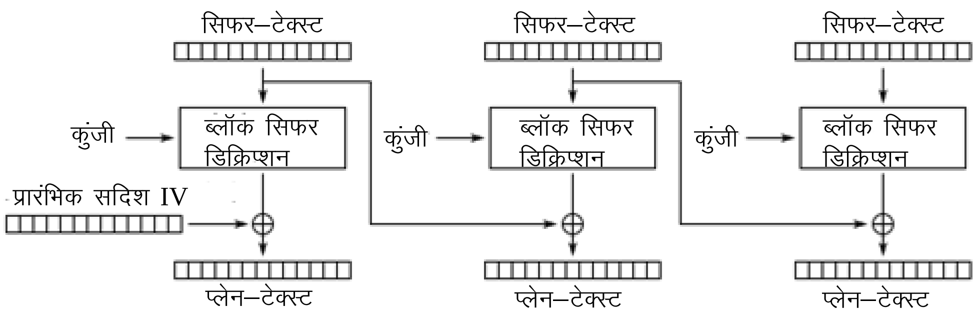
- ➢ CBC, n बिट्स से अधिक इनपुट के लिए अच्छी तरह से काम करता है।
- ➢ CBC एक अच्छा प्रमाणीकरण तंत्र है।
- ➢ ECB की तुलना में क्रिप्टैनालिसिस (कूटविश्लेषण) के प्रति बेहतर प्रतिरोधक प्रकृति।

CBC के नुकसानः

- ➢ समानांतर एन्क्रिप्शन संभव नहीं है क्योंकि हर एन्क्रिप्शन को पिछले सिफर की आवश्यकता होती है।



(चित्र क्र0 4.5: सिफर ब्लॉक चेनिंग (CBC) मोड एन्क्रिप्शन)



(चित्र क्र0 4.6: सिफर ब्लॉक चेनिंग (CBC) मोड डिक्रिप्शन)

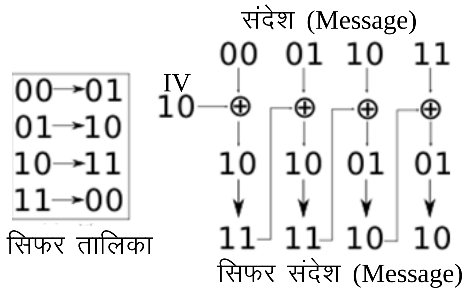
यदि प्रथम ब्लॉक में इंडेक्स 1 है, तो CBC एन्क्रिप्शन का गणितीय फॉर्मूला हैः

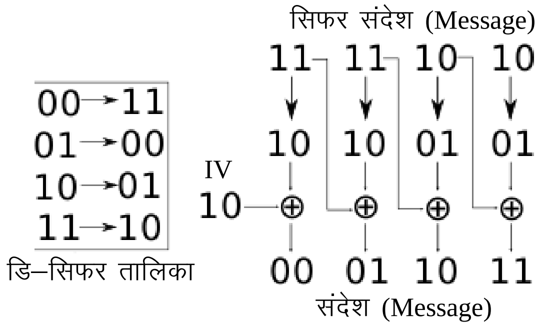
$$C_i = E_k(P_i \oplus C_{i-1})$$
$$C_0 = IV$$

जबकि CBC डिक्रिप्शन के लिए गणितीय सूत्र हैः

$$P_i = D_k(C_i) \oplus C_{i-1}$$
$$C_0 = IV$$

उदाहरण:





CBC संक्रिया का सबसे अधिक उपयोग किया जाने वाला विधि है। इसका मुख्य दोष यह है कि एन्क्रिप्शन अनुक्रमिक है (अर्थात्, इसे समानांतर नहीं किया जा सकता है), और यह कि संदेश को सिफर ब्लॉक (कूटलेख खण्ड) आकार के एक से अधिक में पैडेड किया जाना चाहिए। इस अंतिम स्थिति को संभालने की एक विधि सिफर–टेक्स्ट (कूटलेख–पाठ) चोरी के रूप में जाना जाता है। स्मरण रहे कि एक प्लेन–टेक्स्ट (साधारण–पाठ) या आरंभीकरण सदिश (IV) में एक–सा परिवर्तन सभी सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को प्रभावित करता है।

त्रुटिपूर्ण IV के साथ डिक्रिप्ट करने से प्लेन–टेक्स्ट (साधारण–पाठ) का पहला ब्लॉक दूषित हो जाता है लेकिन बाद में प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक सही हो जाएगा। ऐसा इसलिए है क्योंकि प्रत्येक ब्लॉक पूर्व ब्लॉक के सिफर–टेक्स्ट (कूटलेख–पाठ) के साथ XORed है, प्लेन–टेक्स्ट (साधारण–पाठ) नहीं, इसलिए किसी को वर्तमान के डिक्रिप्शन के लिए IV के रूप में उपयोग करने से पहले पूर्व ब्लॉक को डिक्रिप्ट करने की आवश्यकता नहीं है। इसका अर्थ यह है कि एक प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को सिफर–टेक्स्ट (कूटलेख–पाठ) के दो आसन्न (adjacent) ब्लॉक से पुनः प्राप्त किया जा सकता है।

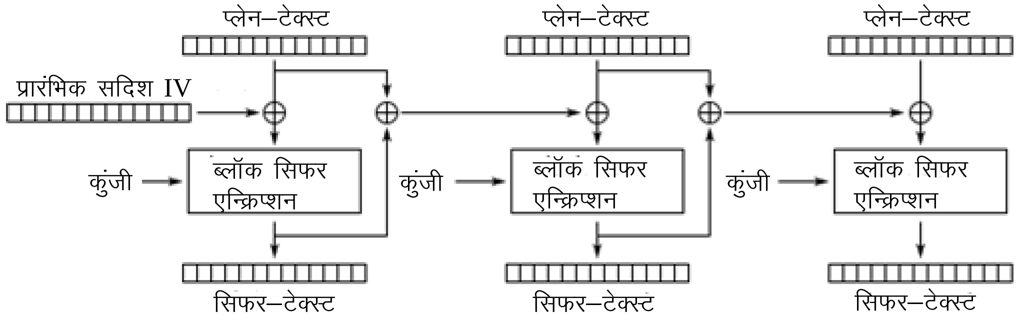
परिणामस्वरूप, डिक्रिप्शन को समानांतर किया जा सकता है। स्मरण रहे कि सिफर–टेक्स्ट (कूटलेख–पाठ) में एक–बिट परिवर्तन के कारण प्लेन–टेक्स्ट (साधारण–पाठ) के संगत ब्लॉक पूर्ण दूषित हो जाता है, और प्लेन–टेक्स्ट (साधारण–पाठ) के निम्नलिखित ब्लॉक में संबंधित बिट को इन्वर्ट करता है, लेकिन शेष ब्लॉक अक्षुण्ण रहते हैं। इस विशेषता का शोषण POODLE जैसे विभिन्न पैडिंग ओरेकल हमलों में किया जाता है।

स्पष्ट आरंभिक सदिश, एक एकल यादृच्छिक ब्लॉक को प्लेन–टेक्स्ट (साधारण–पाठ) से जोड़कर इस गुण का लाभ उठाते हैं। एन्क्रिप्शन सामान्य रूप से किया जाता है, केवल IV को डिक्रिप्शन नैत्य के लिए संचार करने की आवश्यकता नहीं है। जब भी IV डिक्रिप्शन उपयोग किया जाता है, केवल यादृच्छिक ब्लॉक दूषित होता है। यह सुरक्षित रूप से पृथक किया जा सकता है और शेष डिक्रिप्शन मूल प्लेन–टेक्स्ट (साधारण–पाठ) है।

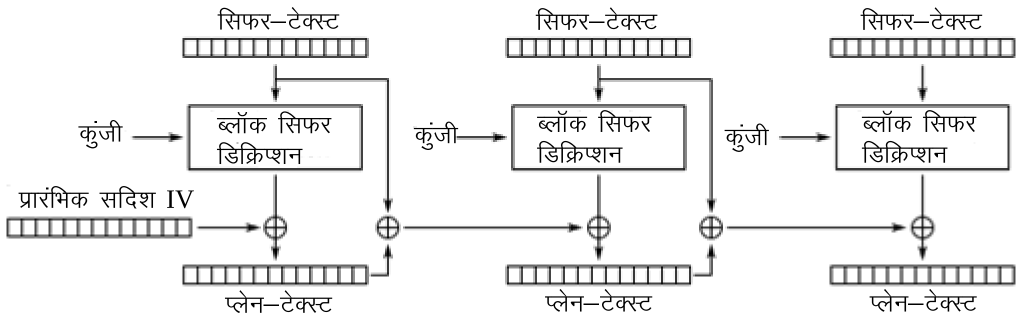
सिफर ब्लॉक चेनिंग का विस्तार (PCBC):

सिफर ब्लॉक चेनिंग का विस्तार या प्लेन–टेक्स्ट (साधारण–पाठ) सिफर–ब्लॉक चैनिंग मोड सिफर–टेक्स्ट (कूटलेख–पाठ) में छोटे परिवर्तन के कारण बनता है, जिसे डिक्रिप्ट (अकूटित) करते समय अनिश्चित काल तक विस्तारित किया जाता है, जब एन्क्रिप्ट (कूटित) किया जाता है।

PCBC मोड में, प्लेन–टेक्स्ट (साधारण–पाठ) का प्रत्येक ब्लॉक पिछले प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक और एन्क्रिप्टेड होने से पहले पूर्व सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक दोनों के साथ XORed है। CBC मोड के साथ, प्रथम ब्लॉक में एक आरंभीकरण सदिश का उपयोग किया जाता है।



(चित्र क्र0 4.7: PCBC मोड एन्क्रिप्शन)



(चित्र क्र0 4.8: PCBC मोड डिक्रिप्शन)

एन्क्रिप्शन और डिक्रिप्शन एल्गोरिथम (कलनविधि) इस प्रकार हैं:

$$C_i = E_k(P_i \oplus P_{i-1} \oplus C_{i-1}),\ P_0 \oplus C_0 = IV$$

$$P_i = D_k(C_i) \oplus P_{i-1} \oplus C_{i-1},\ P_0 \oplus C_0 = IV$$

PCBC का उपयोग Kerberos v4 और WASTE में किया जाता है, सबसे विशेष रूप से, लेकिन अन्यथा सार्व नहीं है। PCBC मोड में एन्क्रिप्ट (कूटित) किए गए संदेश पर, यदि दो आसन्न सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक का आदान–प्रदान किया जाता है, तो यह बाद के ब्लॉक के डिक्रिप्शन को प्रभावित नहीं करता है। इस कारण से, Kerberos v5 में PCBC का उपयोग नहीं किया जाता है।

4.3 सिफर (कूटलेख) फीडबैक मोड (CFB):

इस मोड में, प्रत्येक सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को अगले प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को एन्क्रिप्ट (कूटित) करने के लिए एन्क्रिप्शन प्रक्रिया में फेड बैक मिलता है।

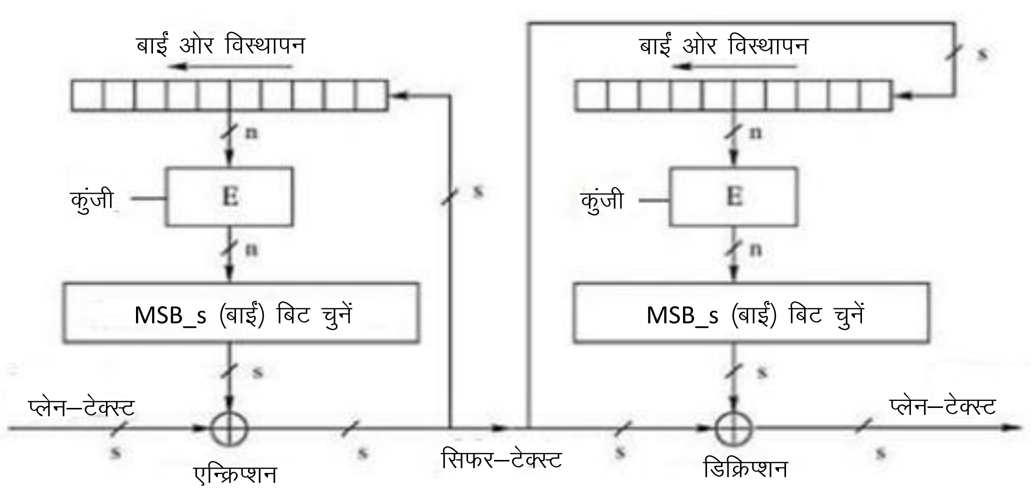
CFB के लाभ:

- चूंकि, शिफ्ट (विस्थापन) रजिस्टर के उपयोग के कारण कुछ डेटा हानि होती है, इसलिए क्रिप्टोनालिसिस (कूटविश्लेषण) लागू करना कठिन है।

संक्रिया:

CFB मोड के संचालन को निम्न चित्रण में दर्शाया गया है। उदाहरण के लिए, वर्तमान प्रणाली में, एक संदेश खंड का आकार s बिट्स है जहाँ $1 < s < n$ है। CFB मोड के लिए प्रारंभिक यादृच्छिक n–बिट इनपुट ब्लॉक के रूप में आरंभीकरण सदिश (IV) की आवश्यकता होती है। IV को गुप्त नहीं होना चाहिए। संक्रिया के चरण हैं –

- IV को शीर्ष रजिस्टर में लोड करें।
- कुंजी K तथा अंतर्निहित ब्लॉक सिफर (खण्ड कूटलेख) के साथ शीर्ष रजिस्टर में डेटा मान को एन्क्रिप्ट (कूटित) करें।
- एन्क्रिप्शन प्रक्रिया के आउटपुट के MSB (Most Significant Bits) अर्थात् बायां बिट की केवल s संख्या लें और सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक उत्पन्न करने के लिए उन्हें s बिट प्लेन–टेक्स्ट (साधारण–पाठ) संदेश के साथ XOR करें।
- पहले से उपलब्ध डेटा को बाईं ओर स्थानांतरित करके शीर्ष रजिस्टर में सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक फीड करें और तब तक संक्रिया जारी रखें जब तक सभी प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक संसाधित नहीं हो जाते।
- अनिवार्य रूप से, पिछले सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक को कुंजी के साथ एन्क्रिप्ट (कूटित) किया गया है, और फिर परिणाम को वर्तमान प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक पर XORed किया गया है।
- डिक्रिप्शन के लिए इसी तरह के चरणों का पालन किया जाता है। पहले से तय की गई IV को डिक्रिप्शन के आरंभ में लोड कर दिया जाता है।



(चित्र क्र0 4.9)

CFB मोड का विशलेषण:

CFB मोड ECB मोड से काफी भिन्न होता है, दिए गए प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक के संगत सिफर–टेक्स्ट (कूटलेख–पाठ) न केवल उस प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक और कुंजी पर निर्भर करता है, बल्कि पिछले सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक पर भी निर्भर करता है। अन्य शब्दों में, सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक संदेश पर निर्भर है।

CFB में एक बहुत ही पृथक विशेषता है। इस मोड में, उपयोगकर्ता ब्लॉक सिफर (खण्ड कूटलेख) की केवल एन्क्रिप्शन प्रक्रिया का उपयोग करके सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट (अकूटित) करता है। अंतर्निहित ब्लॉक सिफर (खण्ड कूटलेख) के डिक्रिप्शन एल्गोरिथ्म (कलनविधि) का उपयोग कभी नहीं किया जाता है।

स्पष्ट है, CFB मोड एक ब्लॉक सिफर (खण्ड कूटलेख) को एक प्रकार की स्ट्रीम सिफर (प्रवाह कूटलेख) में परिवर्तित कर रहा है। एन्क्रिप्शन एल्गोरिथ्म (कलनविधि) की–स्ट्रीम (कुंजी–प्रवाह) उत्पन्न करने के लिए एक की–स्ट्रीम (कुंजी–प्रवाह) जनित्र के रूप में उपयोग किया जाता है जिसे नीचे रजिस्टर में रखा गया है। यह की–स्ट्रीम (कुंजी–प्रवाह) तब प्लेन–टेक्स्ट (साधारण–पाठ) के साथ XORed है जैसा कि स्ट्रीम सिफर (प्रवाह कूटलेख) की दशा में।

ब्लॉक सिफर (खण्ड कूटलेख) को एक स्ट्रीम सिफर (प्रवाह कूटलेख) में परिवर्तित करके, CFB मोड एक ब्लॉक सिफर (खण्ड कूटलेख) के लाभकारी गुणों को बनाए रखते हुए स्ट्रीम सिफर (प्रवाह कूटलेख) के कुछ लाभकारी गुण प्रदान करता है। ब्लॉक बदलने के कारण, फ्लिप की ओर, प्रसारण की त्रुटि प्रचारित हो जाती है।

CFB मोड का CBC मोड से नजदीकी संबंध होता है, जो एक ब्लॉक सिफर (खण्ड कूटलेख) को सेल्फ–सिन्क्रोनाइजिंग स्ट्रीम सिफर बनाता है। संक्रिया बहुत समान है, विशेष रूप से, CFB डिक्रिप्शन लगभग CBC एन्क्रिप्शन के समान है जो व्युत्क्रम में किया जाता है।

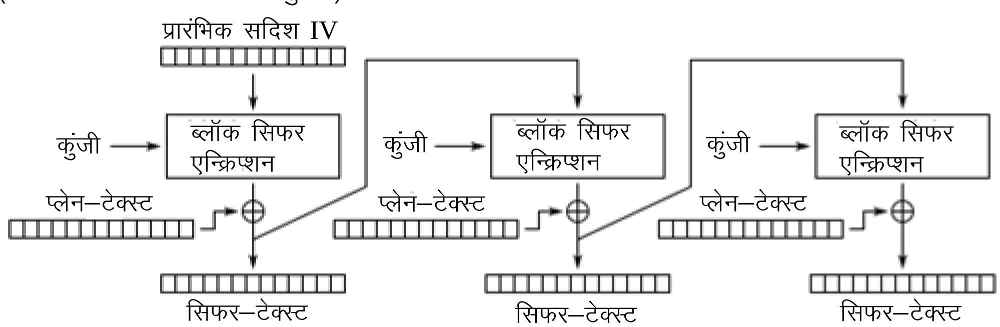
सेल्फ–सिन्क्रोनाइजिंग सिफर की परिभाषा के अनुसार, यदि सिफर–टेक्स्ट (कूटलेख–पाठ) का भाग खो जाता है (जैसे ट्रांसमिशन त्रुटियों के कारण), तो प्राप्तकर्त्ता मूल संदेश का कुछ भाग (विकृत सामग्री) खो देगा, और इसे सही ढंग से स्थानांतरित करने के लिए जारी रखने में सक्षम होना चाहिए, कुछ मात्रा में इनपुट डेटा को संसाधित करने के बाद शेष ब्लॉक को।

ऊपर वर्णित CFB का उपयोग करने का सबसे सरल तरीका सेल्फ–सिन्क्रोनाइजेशन नहीं है। केवल अगर सिफर–टेक्स्ट (कूटलेख–पाठ) का एक पूरा ब्लॉक खो गया है तो CFB सिन्क्रोनाइज हो जाएगा, लेकिन केवल एक बाइट या बिट खोने से स्थायी रूप से डिक्रिप्शन बंद हो जाएगा।

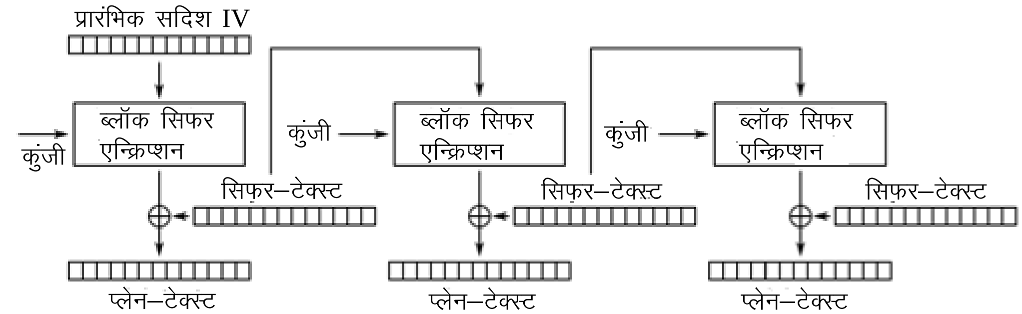
केवल एक बाइट या बिट की हानि के उपरांत सन्क्रोनाइज करने में सक्षम होने के लिए, एक बार में एक बाइट या बिट को एन्क्रिप्ट (कूटित) किया जाना चाहिए। CFB का उपयोग इस तरह से किया जा सकता है कि जब इसे ब्लॉक सिफर (खण्ड कूटलेख) के इनपुट के रूप में शिफ्ट रजिस्टर के साथ जोड़ा जाता है।

CFB का उपयोग कर एक सेल्फ–सिन्क्रोनाइजिंग स्ट्रीम सिफर (प्रवाह कूटलेख) बनाने के लिए जो खोए हुए x बिट्स के किसी भी गुणत के लिए सिन्क्रोनाइज करेगा, एक शिफ्ट रजिस्टर को आरंभीकृत करके ब्लॉक आकार के आकार को आरंभीकरण सदिश के साथ पंजीकृत करें।

इसे ब्लॉक सिफर (खण्ड कूटलेख) के साथ एन्क्रिप्ट (कूटित) किया गया है, और सिफर–टेक्स्ट (कूटलेख–पाठ) के x बिट्स को जनित करने के लिए एन्क्रिप्ट (कूटित) परिणाम के उच्चतम x बिट्स को प्लेन–टेक्स्ट (साधारण–पाठ) के x बिट्स के साथ XOR'ed किया गया है। आउटपुट के इन x बिट्स को शिफ्ट रजिस्टर में स्थानांतरित कर दिया जाता है, और प्रक्रिया (ब्लॉक सिफर के साथ शिफ्ट रजिस्टर को एन्क्रिप्ट करने के आरंभ के साथ) की प्लेन–टेक्स्ट (साधारण–पाठ) के अगले x बिट्स के लिए पुनरावृत्ति की जाती है। डिक्रिप्शन समान है, आरंभीकरण सदिश के साथ आरंभ करें, एन्क्रिप्ट (कूटित) करें और प्लेन–टेक्स्ट (साधारण–पाठ) के x बिट्स को जनित करने के लिए सिफर–टेक्स्ट (कूटलेख–पाठ) के x बिट्स के साथ परिणाम को XOR करें, तब सिफर–टेक्स्ट (कूटलेख–पाठ) के x बिट्स को शिफ्ट रजिस्टर में स्थानान्तरित करें और पुनः एन्क्रिप्ट (कूटित) करें। इस विधि को CFB-8 या CFB-1 (स्थानांतरण के आकार के अनुसार) के रूप में जाना जाता है।



(चित्र क्र0 4.10: CFB मोड एन्क्रिप्शन)



(चित्र क्र0 4.11: CFB मोड डिक्रिप्शन)

संकेतन में, जहाँ S_i शिफ्ट रजिस्टर की iवीं अवस्था है, a << x, x बिट्स स्थानांतरित होता है, head (a, x), a का x उच्चतम बिट्स है, और n, IV के बिट्स की संख्या है।

यदि x बिट्स सिफर–टेक्स्ट (कूटलेख–पाठ) से खो जाते हैं, तो सिफर (कूटलेख) गलत प्लेन–टेक्स्ट (साधारण–पाठ) का उत्पादन करेगा, जब तक कि शिफ्ट रजिस्टर एक बार फिर से एनक्रिप्ट (कूटित) करते समय आयोजित की गई अवस्था के बराबर नहीं हो जाता है, जिस बिन्दु पर सिफर (कूटलेख) को पुनः सिन्क्रोनाइज (तुल्यकालन) किया गया है। यह आउटपुट के n/s ब्लॉक आकार में परिणाम देगा जो ब्लॉक आकार n के साथ गलत परिणाम है और s स्थानांतरित होने वाले बिट्स की मात्रा है।

CBC मोड के समान, प्लेन–टेक्स्ट (साधारण–पाठ) में परिवर्तन सिफर–टेक्स्ट (कूटलेख–पाठ) में गलत परिणाम देता है, और एन्क्रिप्शन को समानांतर नहीं किया जा सकता है। CBC के समान, डिक्रिप्शन भी समानांतर किया जा सकता है। जब डिक्रिप्टिंग (अकूट प्रक्रिया) होती है, तो सिफर–टेक्स्ट (कूटलेख–पाठ) में एक–बिट परिवर्तन दो प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को प्रभावित करता हैः संगत प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक में एक–बिट परिवर्तन और अगले प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक का पूरा परिवर्तन। बाद में प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को सामान्य रूप से डिक्रिप्ट (अकूटित) किया जाता है।

स्ट्रीम–सिफर (प्रवाह कूटलेख) मोड OFB तथा CTR के साथ CFB मोड, CBC मोड पर दो लाभ की भागीदारी करता हैः ब्लॉक सिफर (खण्ड कूटलेख) का उपयोग केवल एन्क्रिप्टिंग (कूट प्रक्रिया) दिशा में किया जाता है, और संदेश को सिफर ब्लॉक (कूटलेख खण्ड) आकार के एक से अधिक के लिए पैडेड होने की आवश्यकता नहीं है (हालांकि सिफर–टेक्स्ट की चोरी पैडिंग को अनावश्यक बनाने के लिए भी उपयोग किया जाता है)।

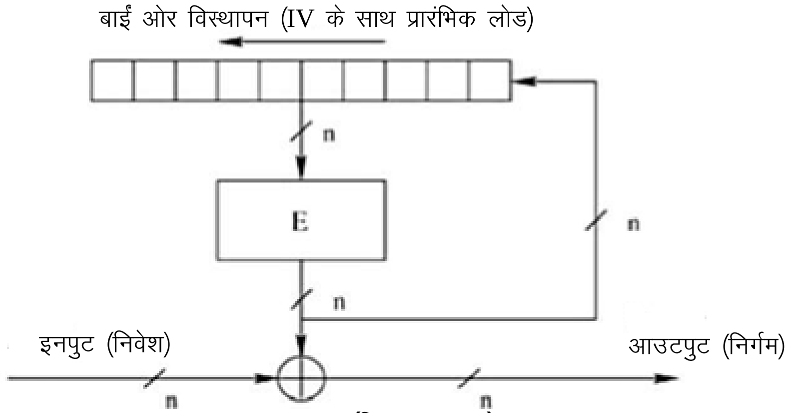
4.4 आउटपुट फीडबैक मोड (OFB) :

इसमें अंतर्निहित ब्लॉक सिफर (खण्ड कूटलेख) से उत्तरोत्तर आउटपुट ब्लॉक्स को वापस फीड करना शामिल है। ये फीडबैक ब्लॉक एन्क्रिप्शन एल्गोरिथ्म (कलनविधि) को प्रविष्ट करने के लिए बिट्स के स्ट्रिंग प्रदान करते हैं जो कि CFB मोड की दशा में की–स्ट्रीम (कुंजी–प्रवाह) जनित्र के रूप में कार्य करते हैं।

जनित की गई कुंजी–स्ट्रीम (कुंजी–प्रवाह) प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक्स के साथ XOR-ed है। OFB मोड के लिए प्रारंभिक यादृच्छिक n–बिट इनपुट ब्लॉक के रूप में IV की आवश्यकता होती है। IV को गुप्त नहीं होना चाहिए।

आउटपुट फीडबैक (OFB) मोड एक ब्लॉक सिफर (खण्ड कूटलेख) को एक सिन्क्रोनस (तुल्यकालिक) स्ट्रीम सिफर (प्रवाह कूटलेख) बनाता है। यह की–स्ट्रीम (कुंजी–प्रवाह) ब्लॉक उत्पन्न करता है, जो तब सिफर–टेक्स्ट (कूटलेख–पाठ) प्राप्त करने के लिए प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक के साथ XORed होता है।

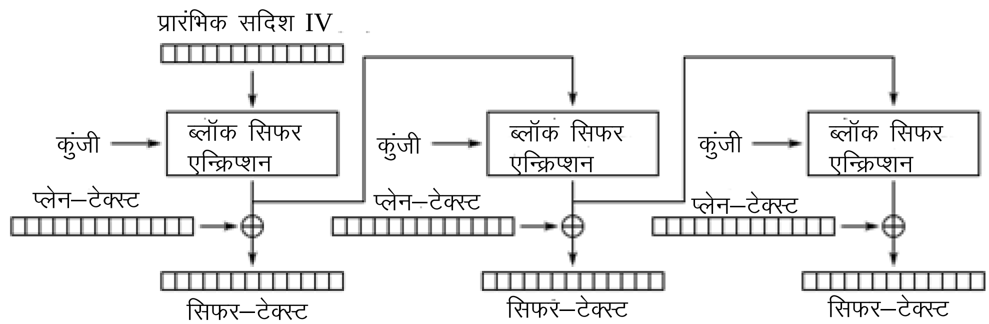
संक्रिया को निम्नलिखित चित्र में दर्शाया गया है –



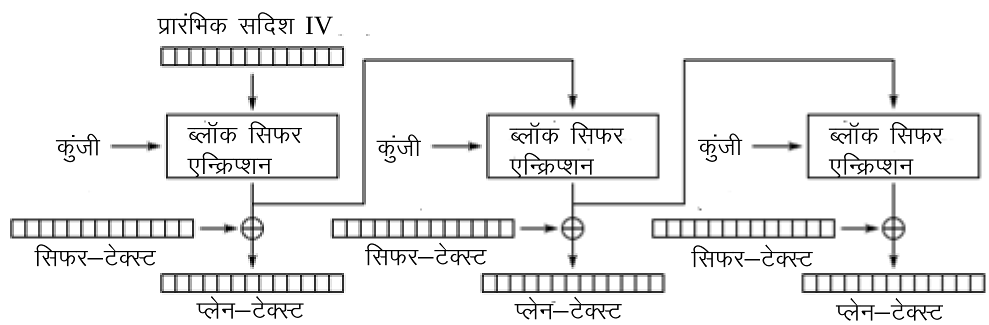
(चित्र क्र0 4.12)

अन्य स्ट्रीम सिफर (प्रवाह कूटलेख) के समान, सिफर–टेक्स्ट (कूटलेख–पाठ) में एक बिट फ्लिप करने से उसी स्थान पर प्लेन–टेक्स्ट (साधारण–पाठ) में फ्लिप बिट उत्पन्न होता है। यह गुण एन्क्रिप्शन से पहले लागू होने पर भी कई त्रुटि कोड को सामान्य रूप से कार्य करने की अनुमति देता है।

XOR ऑपरेशन की समरूपता के कारण, एन्क्रिप्शन और डिक्रिप्शन बिल्कुल समान हैं।



(चित्र क्र0 4.13: OFB मोड एन्क्रिप्शन)



(चित्र क्र0 4.14: OFB मोड डिक्रिप्शन)

प्रत्येक आउटपुट फीडबैक ब्लॉक सिफर (खण्ड कूटलेख) संक्रिया पिछले सभी पर निर्भर करता है, और इसलिए इसे समानांतर में प्रदर्शित नहीं किया जा सकता है। हालाँकि, क्योंकि प्लेन–टेक्स्ट (साधारण–पाठ) या सिफर–टेक्स्ट (कूटलेख–पाठ) का उपयोग केवल अंतिम XOR के लिए किया जाता है, ब्लॉक सिफर (खण्ड कूटलेख) संक्रिया पहले से ही किए जा सकते हैं, अंतिम चरण को प्लेन–टेक्स्ट (साधारण–पाठ) या सिफर–टेक्स्ट (कूटलेख–पाठ) उपलब्ध होने पर समानांतर में प्रदर्शन करने की अनुमति देता है।

इनपुट के रूप में शून्य के स्थिरांक स्ट्रिंग के साथ CBC मोड का उपयोग करके OFB मोड की–स्ट्रीम (कुंजी–प्रवाह) प्राप्त करना संभव है। यह उपयोगी हो सकता है, क्योंकि यह OFB मोड एन्क्रिप्शन के लिए CBC मोड के तीव्र हार्डवेयर कार्यान्वयन के उपयोग की अनुमति देता है।

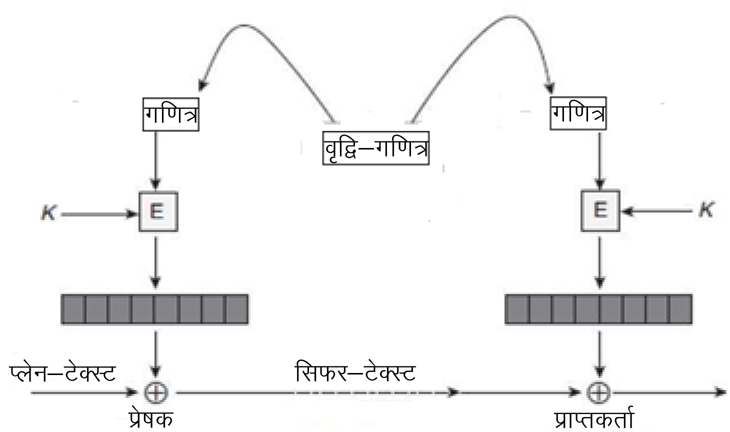
CFB मोड की तरह फीडबैक के रूप में आंशिक ब्लॉक के साथ OFB मोड का उपयोग करने से चक्र की औसत लंबाई 2^{32} या अधिक हो जाती है। डेविस और पार्किन द्वारा प्रस्तावित एक गणितीय मॉडल और प्रायोगिक परिणामों से प्रमाणित होने से पता चलता है कि पूर्ण फीडबैक के साथ केवल एक औसत चक्र की लंबाई जो प्राप्य अधिकतम के करीब हो सकती है। इस कारण से, OFB के विनिर्देशन से काटे गए फीडबैक के लिए समर्थन हटा दिया गया था।

4.5 काउन्टर (गणित्र) मोड (CTR):

इसे फीडबैक के बिना CFB मोड के काउंटर (गणित्र) आधारित संस्करण के रूप में माना जा सकता है। इस मोड में, प्रेषक और प्राप्तकर्त्ता दोनों को एक विश्वसनीय काउंटर (गणित्र) तक पहुंचने की आवश्यकता होती है, जो एक सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक का आदान–प्रदान होने पर प्रत्येक बार एक नए साझा मान की गणना करता है। यह साझा काउंटर (गणित्र) आवश्यक रूप से एक गुप्त मान नहीं है, लेकिन चुनौती यह है कि दोनों पक्षों को काउंटर (गणित्र) को सिन्क्रोनाइज (तुल्यकालिक) रखना चाहिए।

संक्रियाः CTR मोड में एन्क्रिप्शन और डिक्रिप्शन दोनों को निम्न चित्रण में दर्शाया गया है। संचालन के चरण निम्न हैं –

- शीर्ष रजिस्टर में प्रारंभिक काउंटर (गणित्र) मान लोड करना प्रेषक और रिसीवर दोनों के लिए समान है। यह CFB (और CBC) मोड में IV के समान भूमिका निभाता है।
- कुंजी के साथ काउंटर (गणित्र) की सामग्री को एन्क्रिप्ट (कूटित) करें और परिणाम को नीचे के रजिस्टर में रखें।
- नीचे के रजिस्टर की सामग्री के लिए पहला प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक P1 और XOR लें। इसका परिणाम C1 है। प्राप्तकर्त्ता को C1 भेजें और काउंटर (गणित्र) को अद्यतन करें। काउंटर (गणित्र) अद्यतन CFB मोड में सिफर–टेक्स्ट (कूटलेख–पाठ) फीडबैक को बदल देता है।
- अंतिम प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक को एन्क्रिप्ट (कूटित) किए जाने तक इस विधि को जारी रखें।
- डिक्रिप्शन व्युत्क्रम प्रक्रिया है। सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक काउंटर (गणित्र) मान के एन्क्रिप्टेड (कूटित) सामग्री के उत्पादन के साथ XORed है। एन्क्रिप्शन की दशा में प्रत्येक सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक काउंटर (गणित्र) के डिक्रिप्शन के बाद अद्यतन किया जाता है।



(चित्र क्र0 4.15)

काउंटर (गणित्र) मोड का विश्लेषणः

इसमें संदेश निर्भरता नहीं है और इसलिए एक सिफर–टेक्स्ट (कूटलेख–पाठ) ब्लॉक पिछले प्लेन–टेक्स्ट (साधारण–पाठ) ब्लॉक पर निर्भर नहीं करता है।

CFB मोड के समान, CTR मोड में ब्लॉक सिफर (खण्ड कूटलेख) की डिक्रिप्शन प्रक्रिया सम्मिलित नहीं है। ऐसा इसलिए है क्योंकि CTR मोड वास्तव में ब्लॉक–सिफर (खण्ड कूटलेख) का उपयोग करके एक की–स्ट्रीम (कुंजी–प्रवाह) उत्पन्न करता है, जिसे XOR फलन का उपयोग करके एन्क्रिप्ट (कूटित) किया गया है। अन्य शब्दों में, CTR मोड एक ब्लॉक सिफर (खण्ड कूटलेख) को एक स्ट्रीम सिफर (प्रवाह कूटलेख) में परिवर्तित करता है।

CTR मोड का गंभीर नुकसान यह है कि इसके लिए प्रेषक और प्राप्तकर्त्ता में एक सिन्क्रोनाइज (तुल्यकालिक) काउंटर (गणित्र) की आवश्यकता होती है। सिन्क्रोनाइजेशन (तुल्यकालिक) के नुकसान से प्लेन–टेक्स्ट (साधारण–पाठ) की गलत वापसी होती है। हालाँकि, CTR मोड में CFB मोड के लगभग सभी लाभ हैं। इसके अतिरिक्त, यह ट्रांसमिशन की त्रुटि को बिल्कुल भी प्रचारित नहीं करता है। OFB के समान, काउंटर (गणित्र) मोड एक ब्लॉक सिफर (खण्ड कूटलेख) को एक स्ट्रीम सिफर (प्रवाह कूटलेख) में परिवर्तित कर देता है। यह एक काउंटर (गणित्र) के उत्तरोत्तर मानों को एन्क्रिप्ट (कूटित) करके अगला की–स्ट्रीम (कुंजी–प्रवाह) ब्लॉक उत्पन्न करता है।

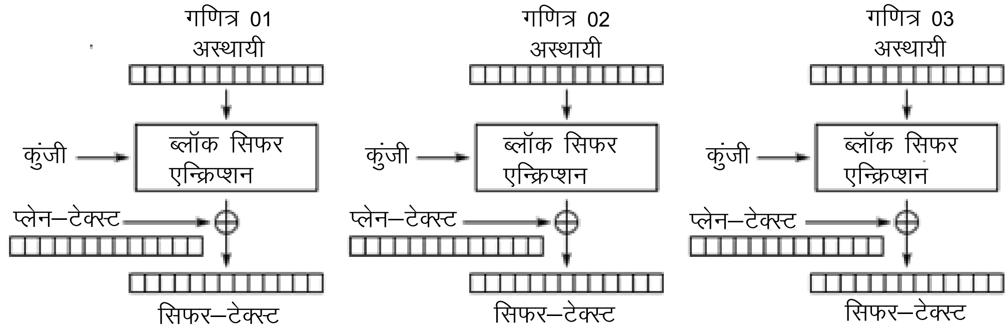
काउंटर (गणित्र) कोई भी फलन हो सकता है जो एक अनुक्रम का उत्पादन करता है और जो लंबे समय तक पुनरावर्तन नहीं करने का आश्वासन देता है, हालांकि एक वास्तविक वेतन वृद्धि–दर काउंटर (गणित्र) सबसे सरल और सबसे लोकप्रिय है। एक साधारण निर्धारक इनपुट (निवेश) फलन का उपयोग विवादास्पद हुआ करता था। आलोचकों ने तर्क दिया कि जानबूझकर एक ज्ञात व्यवस्थित इनपुट (निवेश) के लिए एक क्रिप्टोसिस्टम (कूटतंत्र) को उजागर करना एक अनावश्यक जोखिम का प्रतिनिधित्व करता है। हालांकि, आज CTR मोड को व्यापक रूप से स्वीकार किया जाता है और किसी भी समस्या को अंतर्निहित ब्लॉक सिफर (खण्ड कूटलेख) की कमजोरी माना जाता है, जो इसके इनपुट में प्रणालीगत पूर्वाग्रह की परवाह किए बिना सुरक्षित होने की उम्मीद है। CBC के साथ, CTR मोड नील्स फर्ग्यूसन और ब्रूस श्नेयर द्वारा अनुशंसित दो ब्लॉक सिफर (खण्ड कूटलेख) मोड में से एक है।

CTR मोड को 1979 में व्हिटफील्ड डिफी और मार्टिन हेलमैन द्वारा पेश किया गया था। CTR मोड में OFB की समान विशेषताएं हैं, लेकिन डिक्रिप्शन के समय यह यादृच्छिक पहुँच गुण की भी अनुमति देता है। CTR मोड एक बहु–प्रोसेसर मशीन पर काम करने के लिए अच्छी तरह से अनुकूल है जहां ब्लॉक समानांतर में एन्क्रिप्ट (कूटित) किए जा सकते हैं। इसके अतिरिक्त, यह लघु–चक्र की समस्या से ग्रस्त नहीं है जो OFB को प्रभावित कर सकता है।

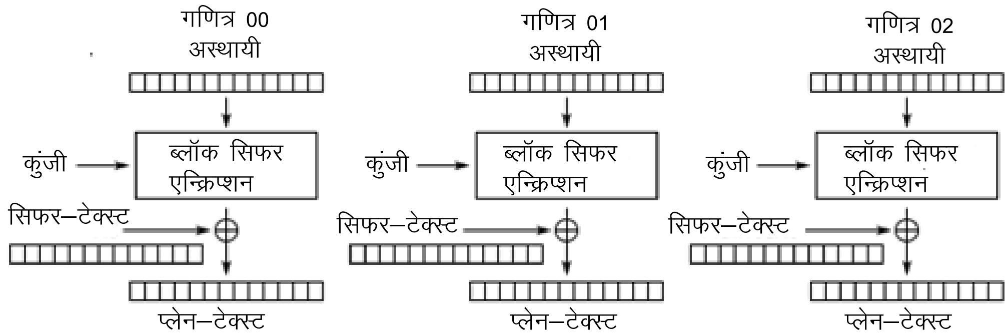
यदि IV अ–यादृच्छिक है, तो उन्हें एन्क्रिप्शन के लिए वास्तविक अद्वितीय काउंटर (गणित्र) ब्लॉक का उत्पादन करने हेतु किसी भी व्युत्क्रम संक्रिया (संयोजन, योग या XOR) का उपयोग करके काउंटर (गणित्र) के साथ जोड़ा जा सकता है। अ–यादृच्छिक (जैसे पैकेट काउंटर) की दशा में, अस्थायी (nonce) और काउंटर (गणित्र) को संयोजित किया जाना चाहिए (जैसे, ऊपरी 64 बिट्स में अस्थायी को संग्रहीत करना और काउंटर (गणित्र) को 128–बिट काउंटर (गणित्र) ब्लॉक के निचले 64 बिट्स में)।

केवल एक ही मान में अस्थायी और काउंटर (गणित्र) को जोड़ने या XORing करने से एक चयनित प्लेन–टेक्स्ट (साधारण–पाठ) हमलावर के तहत कई दशाओं में सुरक्षा भंग हो जाएगी, क्योंकि हमलावर टकराव का कारण बनने के लिए पूरे IV–काउंटर युग्म में हेरफेर करने में सक्षम हो सकता है। एक बार एक हमलावर IV–काउंटर युग्म और प्लेन–टेक्स्ट (साधारण–पाठ) को नियंत्रित करता है, ज्ञात प्लेन–टेक्स्ट (साधारण–पाठ) के साथ सिफर–टेक्स्ट (कूटलेख–पाठ) का XOR एक मान उत्पन्न करेगा, जब उसी IV–काउंटर (गणित्र) युग्म को साझा करने वाले अन्य ब्लॉक के सिफर–टेक्स्ट (कूटलेख–पाठ) के साथ XORed, उस ब्लॉक को डिक्रिप्ट (अकूटित) करेगा।

स्मरण रहे कि इस आरेख में अस्थायी दूसरे आरेखों में आरंभीकरण सदिश (IV) के बराबर है। हालाँकि, यदि ऑफसेट/स्थान की जानकारी त्रुटिपूर्ण है, तो बाइट ऑफसेट पर निर्भरता के कारण इस तरह के डेटा को आंशिक रूप से पुनर्प्राप्त करना असंभव होगा।



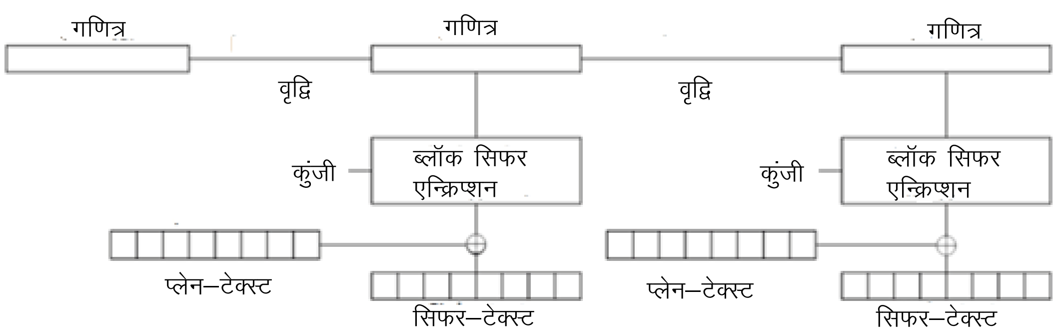
(चित्र क्र0 4.16: CTR मोड एन्क्रिप्शन)



(चित्र क्र0 4.17: CTR मोड डिक्रिप्शन)

गैलोज काउंटर (गणित्र) मोड:

गैलोज काउंटर (गणित्र) मोड (GCM) काउंटर (गणित्र) मोड की एक विशिष्ट दशा है। यह दो मुख्य तरीकों से भिन्न है। पहला यह है कि यह एक अस्थायी का उपयोग नहीं करता है (जैसा कि नीचे चित्र में दिखाया गया है), केवल एक काउंटर (गणित्र) पर निर्भर है। दूसरा यह है कि यह एक संदेश प्रमाणीकरण कोड (MAC) की गणना करता है, जो यह सुनिश्चित करने के लिए साधन प्रदान करता है कि संदेश मार्ग से छेड़छाड़ नहीं किया गया था।



(चित्र क्र0 4.18)

4.6 ब्लॉक सिफर (खण्ड कूटलेख) के लाभ और नुकसान:

ब्लॉक सिफर (खण्ड कूटलेख) के लाभ:

स्ट्रीम सिफर (प्रवाह कूटलेख) की तुलना में ब्लॉक सिफर (खण्ड कूटलेख) का एक लाभ कार्यान्वयन और कम प्रतिबंधात्मक आवश्यकताओं में आसानी है।

चूंकि स्ट्रीम सिफर (प्रवाह कूटलेख) अनिवार्य रूप से एन्क्रिप्शन के लिए एक बार पैड उत्पन्न करते हैं, इसलिए उनके द्वारा उत्पन्न की–स्ट्रीम (कुंजी–प्रवाह) को यादृच्छिक होना चाहिए। ब्लॉक सिफर (खण्ड कूटलेख) का एक अन्य लाभ यह है कि कुछ अखंडता सुरक्षा तंत्र प्रदान करते हैं (जैसे कि GCM मोड में MAC)। यह प्राप्तकर्ता को यह सत्यापित करने की अनुमति देता है कि संदेश पारगमन में छेड़छाड़ नहीं किया गया था।

ब्लॉक सिफर (खण्ड कूटलेख) के नुकसानः

ब्लॉक सिफर (खण्ड कूटलेख) धीमे और स्ट्रीम सिफर (प्रवाह कूटलेख) की तुलना में कम मेमोरी कुशल हैं। चूँकि ब्लॉक सिफर (खण्ड कूटलेख) को किसी दिए गए आकार के ब्लॉक में प्लेन–टेक्स्ट (साधारण–पाठ) को एन्क्रिप्ट (कूटित) करने की आवश्यकता होती है, इसलिए अक्सर प्लेन–टेक्स्ट (साधारण–पाठ) को ब्लॉक लंबाई के एक से अधिक बार पैड करना आवश्यक होता है। यह पैडेड प्लेन–टेक्स्ट (साधारण–पाठ) और सिफर–टेक्स्ट (कूटलेख–पाठ) को संग्रहीत करने के लिए सिफर (कूटलेख) की मेमोरी आवश्यकताओं को बढ़ाता है।

सिफर (कूटलेख) को ब्लॉक करने का एक और नुकसान यह है कि ट्रांसमिशन की त्रुटियां अक्सर शेष सिफर–टेक्स्ट (कूटलेख–पाठ) को अप्राप्य बनाती हैं। स्ट्रीम सिफर (प्रवाह कूटलेख) में, ट्रांसमिशन में एक एकल बिट त्रुटि आमतौर पर डिक्रिप्टेड (अकूटित) प्लेन–टेक्स्ट (साधारण–पाठ) के एक बिट को प्रभावित करता है, जो पुनर्प्राप्त करने योग्य हो सकता है। संक्रिया के फीडबैक मोड का उपयोग करते हुए एक ब्लॉक सिफर (खण्ड कूटलेख) में, ट्रांसमिशन में एक एकल बिट त्रुटि इसके ब्लॉक और प्रत्येक ब्लॉक के डिक्रिप्शन को परिवर्तित कर देती है जिसका डिक्रिप्शन इस पर निर्भर करता है।

अभ्यास

1. इलेक्ट्रॉनिक कोड बुक मोड से क्या समझते हैं?
2. सिफर ब्लॉक (कूटलेख खण्ड) चेनिंग मोड को विस्तार से समझाइए।
3. सिफर (कूटलेख) फीडबैक मोड पर टिप्पणी लिखिए।
4. आउटपुट फीडबैक मोड को संक्षेप में समझाइए।
5. काउन्टर (गणित्र) मोड को विस्तार से समझाइए।
6. ब्लॉक सिफर (खण्ड कूटलेख) के लाभ और नुकसान लिखिए।

अध्याय – 5

पब्लिक की एन्क्रिप्शन
(सार्वजनिक कुंजी कूट प्रक्रिया)

5.1 पब्लिक की क्रिप्टोग्राफी (सार्वजनिक कुंजी कूटेखन):

पब्लिक की क्रिप्टोग्राफी (सार्वजनिक कुंजी कूटेखन), या असममित क्रिप्टोग्राफी (कूटलेखन), एक क्रिप्टोग्राफिक (कूटलेखीय) प्रणाली है जो कुंजियों के युग्म का उपयोग करती हैः सार्वजनिक कुंजी जो व्यापक रूप से प्रचारित की जा सकती है, और व्यक्तिगत कुंजी जो केवल स्वामी को ज्ञात होती है। इस तरह की कुंजी की पीढ़ी एक–तरफा कार्यों का उत्पादन करने के लिए गणितीय समस्याओं पर आधारित क्रिप्टोग्राफिक (कूटलेखीय) एल्गोरिथ्म (कलनविधि) पर निर्भर करती है। प्रभावी सुरक्षा के लिए केवल व्यक्तिगत कुंजी को व्यक्तिगत रखने की आवश्यकता होती है; सार्वजनिक कुंजी को सुरक्षा से समझौता किए बिना खुले तौर पर वितरित किया जा सकता है।

ऐसी प्रणाली में, कोई भी व्यक्ति प्राप्तकर्त्ता की सार्वजनिक कुंजी का उपयोग करके एक संदेश को एन्क्रिप्ट (कूटित) कर सकता है, लेकिन उस एन्क्रिप्ट (कूटित) किए गए संदेश को केवल प्राप्तकर्त्ता की निजी कुंजी के साथ डिक्रिप्ट (अकूटित) किया जा सकता है।

मजबूत प्रमाणीकरण भी संभव है। एक प्रेषक संदेश पर एक संक्षिप्त डिजिटल (अंकीय) हस्ताक्षर बनाने के लिए एक व्यक्तिगत कुंजी के साथ एक संदेश को जोड़ सकता है। संबंधित सार्वजनिक कुंजी वाला कोई भी एक संदेश, उस पर एक स्थानिक डिजिटल (अंकीय) हस्ताक्षर, और यह सत्यापित करने के लिए ज्ञात सार्वजनिक कुंजी को जोड़ सकता है कि क्या हस्ताक्षर मान्य था, अर्थात् संबंधित व्यक्तिगत कुंजी के स्वामी द्वारा बनाया गया था।

सार्वजनिक कुंजी एल्गोरिथ्म (कलनविधि) आधुनिक क्रिप्टोकरंसी, अनुप्रयोग और प्रोटोकॉल (संदेशाचार) में मूलभूत सुरक्षा तत्व हैं जो इलेक्ट्रॉनिक संचार और डेटा भंडारण की गोपनीयता, प्रामाणिकता और गैर–प्रतिक्षेप्यता का आश्वासन देते हैं। वे विभिन्न इंटरनेट मानकों को रेखांकित करते हैं, जैसे ट्रांसपोर्ट लेयर सिक्योरिटी (TLS), S/MIME, PGP और GPG। कुछ सार्वजनिक कुंजी एल्गोरिथ्म (कलनविधि) कुंजी वितरण और गोपनीयता (जैसे, डिफी–हेलमैन कुंजी विनिमय) प्रदान करते हैं, कुछ डिजिटल (अंकीय) हस्ताक्षर (जैसे, डिजिटल हस्ताक्षर एल्गोरिथ्म) प्रदान करते हैं, और कुछ दोनों (जैसे, RSA) प्रदान करते हैं।

1970 के दशक के मध्य से पहले, सभी सिफर (कूटलेख) प्रणाली सममित कुंजी एल्गोरिथ्म (कलनविधि) का उपयोग कर रहे थे, जिसमें प्रेषक और प्राप्तकर्ता दोनों द्वारा अंतर्निहित एल्गोरिथ्म (कलनविधि) के साथ एक ही क्रिप्टोग्राफिक (कूटलेखीय) कुंजी का उपयोग किया जाता है, जिन्हें दोनों को गुप्त रखना होगा। आवश्यकता के अनुसार, इस तरह की प्रत्येक प्रणाली में कुंजी को किसी भी प्रएाली के उपयोग से पहले कुछ सुरक्षित तरीके से संचार दलों के बीच आदान–प्रदान करना पड़ता था – एक सुरक्षित प्रणाली। यह आवश्यकता कभी भी तुच्छ नहीं होती है और बहुत तेजी से असहनीय हो जाती है क्योंकि प्रतिभागियों की संख्या बढ़ जाती है, या जब कुंजी विनिमय के लिए सुरक्षित प्रणाली उपलब्ध नहीं होते हैं, या जब (जैसा कि समझदार क्रिप्टोग्राफिक अभ्यास होता है), कुंजियाँ अक्सर बदल जाती हैं। विशेष रूप से, यदि संदेश अन्य उपयोगकर्ताओं से सुरक्षित हैं, तो उपयोगकर्ताओं की प्रत्येक संभावित जोड़ी के लिए एक पृथक कुंजी आवश्यक है।

इसके विपरीत, एक सार्वजनिक कुंजी प्रणाली में, सार्वजनिक कुंजियों को व्यापक रूप से और खुले रूप से प्रचारित किया जा सकता है – और केवल व्यक्तिगत कुंजी को उसके मालिक द्वारा सुरक्षित रखने की आवश्यकता होती है।

सममित क्रिप्टोग्राफी (कूटलेखन) द्वारा उत्पन्न सुरक्षा परिस्थितियों को संबोधित करने के लिए असममित क्रिप्टोग्राफी (कूटलेखन) नामक दृष्टिकोण विकसित हुआ। यह विधि एक ही कुंजी के स्थान पर दो कुंजी का उपयोग करके गुप्त कुंजी क्रिप्टोग्राफी (कूटलेखन) की समस्या को हल करती है। असममित क्रिप्टोग्राफी (कूटलेखन) कुंजियों की एक जोड़ी का उपयोग करती है। इस प्रक्रिया में, एक कुंजी का उपयोग एन्क्रिप्शन के लिए किया जाता है, और दूसरी कुंजी का उपयोग डिक्रिप्शन के लिए किया जाता है।

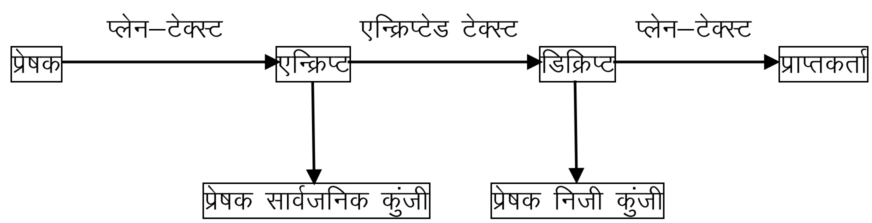
इस प्रक्रिया को असममित क्रिप्टोग्राफी (कूटलेखन) के रूप में जाना जाता है क्योंकि प्रक्रिया को पूरा करने के लिए दोनों कुंजियों की आवश्यकता होती है। इन दोनों कुंजियों को सामूहिक रूप से प्रमुख जोड़ी के रूप में जाना जाता है। असममित क्रिप्टोग्राफी (कूटलेखन) में, कुंजियों में से एक स्वतंत्र रूप से वितरित करने योग्य है।

इस कुंजी को सार्वजनिक कुंजी कहा जाता है और इसका उपयोग एन्क्रिप्शन (कूट प्रक्रिया) के लिए किया जाता है। इसलिए, एन्क्रिप्शन (कूट प्रक्रिया) की इस पद्धति को सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) भी कहा जाता है। दूसरी कुंजी गुप्त या व्यक्तिगत कुंजी है और इसका उपयोग डिक्रिप्शन (अकूट प्रक्रिया) के लिए किया जाता है। व्यक्तिगत कुंजी वितरित करने योग्य नहीं है। यह कुंजी, जैसा कि इसके नाम से पता चलता है, प्रत्येक संचार इकाई के लिए व्यक्तिगत है।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) में, सार्वजनिक कुंजी के साथ एन्क्रिप्ट (कूटित) किया गया डेटा केवल उसी व्यक्तिगत कुंजी के साथ डिक्रिप्ट (अकूटित) किया जा सकता है। इसके विपरीत, व्यक्तिगत कुंजी के साथ एन्क्रिप्ट (कूटित) किया गया डेटा केवल संबंधित सार्वजनिक कुंजी के साथ डिक्रिप्ट (अकूटित) किया जा सकता है। इस विषमता के कारण, सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) को असममित क्रिप्टोग्राफी (कूटलेखन) के रूप में जाना जाता है।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) कैसे कार्य करती है?

आइए देखें कि यह व्यवहार में कैसे कार्य करता है। एक उदाहरण पर विचार करें, जहाँ प्रेषक (sender) प्राप्तकर्त्ता (receiver) को एक एन्क्रिप्टेड (कूटित) फाइल भेजना चाहता है। इस स्थिति में, प्राप्तकर्त्ता एक जोड़ी कुंजी प्राप्त करेगा, निजी कुंजी को बनाए रखेगा और सार्वजनिक कुंजी वितरित करेगा। इसलिए, प्रेषक के पास प्राप्तकर्त्ता की सार्वजनिक कुंजी की एक प्रति है। प्रेषक तब प्राप्तकर्त्ता की सार्वजनिक कुंजी का उपयोग करके फाइल को एन्क्रिप्ट (कूटित) करता है और एन्क्रिप्ट (कूटित) की गई फाइल को प्राप्तकर्त्ता को भेजता है। चूंकि कुंजी के युग्म पूरक हैं, केवल प्राप्तकर्त्ता की निजी कुंजी इस फाइल को डिक्रिप्ट (अकूटित) कर सकती है। यदि कोई अन्य व्यक्ति फाइल को स्वीकार करता है, तो वे फाइल को डिक्रिप्ट (अकूटित) नहीं कर पाएंगे, क्योंकि डिक्रिप्शन (अकूटन) के लिए केवल प्राप्तकर्त्ता की निजी कुंजी का उपयोग किया जा सकता है। निम्नलिखित चित्र सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) की प्रक्रिया की व्याख्या करता है।



(चित्र क्र0 5.1)

सार्वजनिक कुंजी एन्क्रिप्शन (कूटन):

यह विधि बहुत स्पष्ट रूप से इंगित करती है कि हमारे द्वारा उपयोगकर्ता को भेजा जाने वाला डेटा केवल सार्वजनिक कुंजी द्वारा एन्क्रिप्ट (कूटित) किया जा सकता है। इसी तरह, डिक्रिप्शन (अकूट प्रक्रिया) केवल व्यक्तिगत कुंजी द्वारा किया जा सकता है, जो डेटा प्राप्तकर्ता द्वारा आपूर्ति की जाती है। इसलिए, पारगमन में डेटा किसी अन्य व्यक्ति द्वारा पहुँच या छेड़छाड़ किए जाने की बहुत कम संभावना है।

इसलिए, संदेशों का सुरक्षित रूप से आदान–प्रदान किया जा सकता है। प्रेषक और प्राप्तकर्त्ता को एक कुंजी साझा करने की आवश्यकता नहीं है, जैसा कि सममित एन्क्रिप्शन (कूट प्रक्रिया) के लिए आवश्यक है। सभी संचारों में केवल सार्वजनिक कुंजी शामिल होती है, और कोई भी व्यक्तिगत कुंजी कभी भी प्रेषित या साझा नहीं की जाती है।

उपरोक्त तंत्र भी इस बात को सामने लाता है कि प्रत्येक प्राप्तकर्ता के पास एक अद्वितीय कुंजी होगी जिसका उपयोग वह अपने समकक्ष सार्वजनिक कुंजी द्वारा एन्क्रिप्ट (कूटित) किए गए डेटा को डिक्रिप्ट (अकूटित) करने के लिए करेगा। डिफी और हेलमैन ने पहले असममित क्रिप्टोग्राफी (कूटलेखन) की प्रक्रिया पर चर्चा की। इस प्रक्रिया का सबसे सार्व कार्यान्वयन RSA एल्गोरिथ्म (कलनविधि) है।

सममित कुंजी क्रिप्टोग्राफी के विपरीत, हमें सार्वजनिक–कुंजी क्रिप्टोग्राफी का ऐतिहासिक उपयोग नहीं मिलता है। यह अपेक्षाकृत नई अवधारणा है।

सममितीय क्रिप्टोग्राफी (कूटलेखन) सरकारों, सेना, और बड़े वित्तीय निगमों जैसे संगठनों के लिए उपयुक्त थी जो वर्गीकृत संचार में शामिल थे।

पिछले कुछ दशकों में अधिक असुरक्षित कम्प्यूटर नेटवर्क के प्रसार के साथ, बड़े पैमाने पर क्रिप्टोग्राफी (कूटलेखन) का उपयोग करने के लिए एक वास्तविक आवश्यकता महसूस की गई थी। मुख्य प्रबंधन के लिए चुनौतियों का सामना करने के कारण सममित कुंजी को गैर–व्यावहारिक पाया गया था। इसने सार्वजनिक कुंजी क्रिप्टोसिस्टम (कूटतंत्र) को जन्म दिया।

सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) योजना के सबसे महत्वपूर्ण गुण निम्न हैं:

- एन्क्रिप्शन (कूट प्रक्रिया) और डिक्रिप्शन (अकूट प्रक्रिया) के लिए विभिन्न कुंजियों का उपयोग किया जाता है। यह एक गुण है जो इस योजना को सममित एन्क्रिप्शन (कूट प्रक्रिया) योजना से पृथक करती है।
- प्रत्येक प्राप्तकर्ता के पास एक अद्वितीय डिक्रिप्शन (अकूट प्रक्रिया) कुंजी होती है, जिसे आमतौर पर उसकी व्यक्तिगत कुंजी कहा जाता है।
- प्राप्तकर्ता को एक एन्क्रिप्शन (कूट प्रक्रिया) कुंजी प्रकाशित करने की आवश्यकता होती है, जिसे उसकी सार्वजनिक कुंजी कहा जाता है।
- प्राप्तकर्ता के रूप में विरोधी द्वारा स्पूफिंग से बचने के लिए एक सार्वजनिक कुंजी की प्रामाणिकता का कुछ आश्वासन इस योजना में आवश्यक है। आम तौर पर, इस प्रकार के क्रिप्टोसिस्टम (कूटतंत्र) में विश्वसनीय तृतीय पक्ष सम्मिलित होता है जो प्रमाणित करता है कि एक विशेष सार्वजनिक कुंजी केवल किसी विशिष्ट व्यक्ति या संस्था से संबंधित है।
- एन्क्रिप्शन (कूट प्रक्रिया) एल्गोरिथ्म (कलनविधि) जटिल है, जो हमलावर को प्लेन–टेक्स्ट (साधारण–पाठ) से सिफर–टेक्स्ट (कूटलेख–पाठ) और एन्क्रिप्शन (कूट प्रक्रिया) कुंजी को हटाने से प्रतिबंधित करता है।
- यद्यपि व्यक्तिगत और सार्वजनिक कुंजी गणितीय रूप से संबंधित हैं, लेकिन सार्वजनिक कुंजी से निजी कुंजी की गणना करना संभव नहीं है। वास्तव में, किसी भी सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटतंत्र) का बुद्धिमान भाग दो कुंजियों के मध्य संबंध बनाना है।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) के लाभः

सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया), जिसमें एक संदेश प्राप्तकर्ता के सार्वजनिक कुंजी के साथ एन्क्रिप्ट (कूटित) किया गया है। इस संदेश को किसी के द्वारा डिक्रिप्ट (अकूटित) नहीं किया जा सकता है, जिसके पास मिलान निजी कुंजी नहीं है, जो इस प्रकार उस कुंजी का स्वामी और सार्वजनिक कुंजी से संबद्ध व्यक्ति माना जाता है। इसका उपयोग गोपनीयता सुनिश्चित करने के प्रयास में किया जाता है।

डिजिटल (अंकीय) हस्ताक्षर, जिसमें एक संदेश को प्रेषक की व्यक्तिगत कुंजी के साथ हस्ताक्षरित किया जाता है और इसे किसी ऐसे व्यक्ति द्वारा सत्यापित किया जा सकता है जिसके पास प्रेषक की सार्वजनिक कुंजी है। यह सत्यापित करता है कि प्रेषक के पास व्यक्तिगत कुंजी तक पहुँच थी, और इसलिए सार्वजनिक कुंजी से जुड़े व्यक्ति होने की संभावना है। यह भी सुनिश्चित करता है कि संदेश के साथ छेड़छाड़ नहीं की गई है, क्योंकि हस्ताक्षर गणितीय रूप से उस संदेश के लिए बाध्य है जिसे मूल रूप से बनाया गया था, और सत्यापन व्यावहारिक रूप से किसी अन्य संदेश के लिए विफल हो जाएगा, चाहे वह मूल संदेश के समान ही क्यों न हो।

सार्वजनिक कुंजी क्रिप्टोग्राफी द्वारा प्रदान की गई डेटा सुरक्षा इसका मुख्य लाभ है। सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) सबसे सुरक्षित प्रोटोकॉल (संदेशाचार) बनी हुई है क्योंकि उपयोगकर्ताओं को कभी भी किसी को अपनी व्यक्तिगत कुंजी प्रेषित या प्रकट करने की आवश्यकता नहीं होती है, जिससे साइबर अपराधियों को ट्रांसमिशन (संचरण) के समय किसी व्यक्ति की गुप्त कुंजी की खोज करने की संभावना कम होती है।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) भी डिजिटल हस्ताक्षर प्रदान करता है जिसे फिर से तैयार नहीं किया जा सकता है। सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) के लिए प्रत्येक उपयोगकर्ता को अपनी व्यक्तिगत कुंजी की सुरक्षा के लिए जिम्मेदार होना चाहिए, जबकि व्यक्तिगत कुंजी सिस्टम को उपयोगकर्ताओं को गुप्त कुंजी साझा करने की आवश्यकता होती है और शायद ट्रांसमिशन (संचरण) के लिए तीसरे पक्ष पर भी भरोसा होता है। गुप्त कुंजी प्रणाली के साथ, प्रेषकों के लिए यह दावा करना संभव है कि साझा गुप्त कुंजी को प्रक्रिया में सम्मिलित किसी एक पक्ष द्वारा समझौता किया गया था।

एक सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) प्रणाली का सबसे स्पष्ट अनुप्रयोग गोपनीयता प्रदान करने के लिए संचार को एन्क्रिप्ट (कूटित) करने में होता है – एक संदेश जिसे प्राप्तकर्ता की सार्वजनिक कुंजी का उपयोग करके प्रेषक एन्क्रिप्ट करता है, केवल प्राप्तकर्ता की युग्मित व्यक्तिगत कुंजी द्वारा डिक्रिप्ट (अकूटित) किया जा सकता है।

चूंकि असममित कुंजी एल्गोरिथ्म (कलनविधि) लगभग सदैव बहुत अधिक कम्प्यूटेशनल (संगणनीय) रूप से सममित लोगों की तुलना में गहन होते हैं, कई दशाओं में एक की–एक्सचेंज एल्गोरिथ्म (कुंजी–विनिमय कलनविधि) का उपयोग करके एक कुंजी का आदान–प्रदान करना आम है, फिर उस कुंजी और एक सममित कुंजी एल्गोरिथ्म (कलनविधि) का उपयोग करके डेटा संचारित करें। PGP, SSH, और SSL/TLS योजनाओं के परिवार इस प्रक्रिया का उपयोग करते हैं, और इस प्रकार ये हाइब्रिड क्रिप्टो सिस्टम (संकर कूट प्रणाली) कहलाते हैं।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) की चुनौतियाँः

गति को अक्सर सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) से जुड़ी सबसे आम चुनौती के रूप में उद्धृत किया जाता है। वर्तमान में उपलब्ध सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) विधि की तुलना में कई व्यक्तिगत कुंजी क्रिप्टोग्राफी (कूटलेखन) विधियाँ बहुत अधिक तीव्र हैं। सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) के साथ इस चुनौती पर काबू पाने की एक विधि यह है कि इसे सार्वजनिक कुंजी प्रणाली के सुरक्षा लाभ और गुप्त (व्यक्तिगत) कुंजी प्रणाली की गति प्रदान करने के लिए गुप्त कुंजी प्रणालियों के साथ जोड़ा जाए।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) से जुड़ी एक और चुनौती यह है कि यह स्पूफ और समझौता किए गए प्रमाणीकरण अधिकारियों के माध्यम से हमलों के लिए अतिसंवेदनशील है। जब ये हमले होते हैं, तो साइबर अपराधी समझौता किए गए प्राधिकरण से एक सार्वजनिक कुंजी प्रमाणपत्र चुनकर लगभग किसी को भी प्रतिरूपित करते हैं। यह साइबर अपराधियों को एक सार्वजनिक कुंजी को दूसरे उपयोगकर्ता के नाम से जोड़ने की अनुमति देता है।

तीन प्रकार की सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) योजनाएँ हैं। वे निम्न हैं, हम अगले अनुच्छेदों में क्रमशः उनकी चर्चा करेंगे:

1. RSA क्रिप्टोसिस्टम (कूटतंत्र)
2. ElGamal क्रिप्टोसिस्टम (कूटतंत्र)
3. इलिप्टिक कर्व क्रिप्टोग्राफी (अंडाकार वक्र कूटलेखन)

5.2 RSA क्रिप्टोसिस्टम (कूटप्रणाली):

यह क्रिप्टोसिस्टम (कूटप्रणाली) एक प्रारंभिक प्रणाली है। यह आज भी सबसे अधिक कार्यरत क्रिप्टोसिस्टम (कूटप्रणाली) है। इस प्रणाली का आविष्कार तीन विद्वानों रॉन रिवेस्ट, आदि शमीर और लेन एडलमैन द्वारा किया गया था और इसलिए, इसे RSA क्रिप्टोसिस्टम (कूटप्रणाली) कहा जाता है।

हम RSA क्रिप्टोसिस्टम (कूटप्रणाली) के दो पहलुओं को देखेंगे, कुंजी जोड़ी की पीढ़ी और एन्क्रिप्शन–डिक्रिप्शन एल्गोरिथ्म (कलनविधि)।

RSA (Rivest–Shamir–Adleman) प्रथम सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) में से एक है और व्यापक रूप से सुरक्षित डेटा ट्रांसमिशन (संचरण) के लिए उपयोग किया जाता है। ऐसे क्रिप्टोसिस्टम (कूटप्रणाली) में एन्क्रिप्शन (कूट प्रक्रिया) कुंजी सार्वजनिक होती है और यह डिक्रिप्शन (अकूट प्रक्रिया) कुंजी से अलग होती है जिसे गुप्त (व्यक्तिगत) रखा जाता है। RSA में, यह विषमता दो बड़े अभाज्य संख्याओं के उत्पाद के गुणन की व्यावहारिक कठिनाई पर आधारित है, गुणनखण्ड समस्या।

RSA का एक उपयोगकर्ता एक सहायक मान के साथ दो बड़े अभाज्य संख्याओं के आधार पर एक सार्वजनिक कुंजी बनाता है और फिर प्रकाशित करता है। अभाज्य संख्याओं को गुप्त रखना होगा। संदेश को एन्क्रिप्ट (कूटित) करने के लिए कोई भी सार्वजनिक कुंजी का उपयोग कर सकता है, लेकिन वर्तमान में प्रकाशित विधियों के साथ, और यदि सार्वजनिक कुंजी काफी बड़ी है, तो केवल प्रमुख संख्याओं के ज्ञान वाले व्यक्ति संदेश को व्यावहारिक रूप से डिकोड कर सकते हैं। RSA एन्क्रिप्शन (कूट प्रक्रिया) को तोड़कर RSA समस्या के रूप में जाना जाता है।

RSA एक अपेक्षाकृत धीमा एल्गोरिथ्म (कलनविधि) है, और इस वजह से, इसका उपयोग आमतौर पर उपयोगकर्ता डेटा को सीधे एन्क्रिप्ट (कूटित) करने के लिए कम ही करते हैं। अधिक बार, RSA सममित कुंजी क्रिप्टोग्राफी (कूटलेखन) के लिए एन्क्रिप्टेड (कूटित) साझा कुंजी को पारित करता है जो बदले में उच्च गति पर कई एन्क्रिप्शन–डिक्रिप्शन संक्रिया कर सकता है।

RSA एल्गोरिथ्म (कलनविधि) का उपयोग क्यों किया जाता है?

RSA बड़े पूर्णांक को दो बड़े अभाज्य संख्याओं का गुणनफल प्रदान करने में कठिनाई से अपनी सुरक्षा प्राप्त करता है। इन दो संख्याओं को गुणा करना आसान है, लेकिन योग से मूल अभाज्य संख्याओं का निर्धारण या गुणनखंड को आज के सुपर कंप्यूटर का उपयोग करने में लगने वाले समय के कारण अचूक माना जाता है।

सार्वजनिक और व्यक्तिगत कुंजी पीढ़ी एल्गोरिथ्म (कलनविधि) RSA क्रिप्टोग्राफी (कूटलेखन) का सबसे जटिल हिस्सा है। दो बड़े अभाज्य संख्याओं, p और q, राबिन–मिलर प्राइमलिटी टेस्ट एल्गोरिथ्म (Rabin-Miller primality test algorithm) का उपयोग करके उत्पन्न होते हैं। एक मापांक n की गणना p और q को गुणा करके की जाती है। इस संख्या का उपयोग सार्वजनिक और व्यक्तिगत दोनों कुंजियों द्वारा किया जाता है और उनके बीच लिंक प्रदान करता है। इसकी लंबाई, जिसे आम तौर पर बिट्स में व्यक्त किया जाता है, को कुजी की लंबाई कहा जाता है।

सार्वजनिक कुंजी में मापांक n और एक सार्वजनिक प्रतिपादक या घातांक e होते हैं, e सामान्य रूप से 65537 पर व्यवस्थित होता है, क्योंकि यह एक अभाज्य संख्या है जो बहुत बड़ी नहीं है। सार्वजनिक रूप से सभी के साथ साझा किए जाने के रूप में e को गुप्त रूप से चयनित अभाज्य संख्या नहीं होना चाहिए।

व्यक्तिगत कुंजी में मापांक n और व्यक्तिगत घातांक d होते हैं, जो n के टोटिएंट फलन के संबंध में गुणक व्युत्क्रम को खोजने के लिए विस्तारित यूक्लिडियन एल्गोरिथ्म (कलनविधि) का उपयोग करके गणना की जाती है।

संक्रियाः

RSA एल्गोरिथ्म (कलनविधि) में चार चरण शामिल हैंः कुंजी का जनन, कुंजी वितरण, एन्क्रिप्शन (कूट प्रक्रिया) और डिक्रिप्शन (अकूट प्रक्रिया)।

RSA के पीछे एक मूल सिद्धांत यह है कि यह तीन बहुत बड़े धनात्मक पूर्णांक e, d और n को प्राप्त के लिए व्यावहारिक है जो सभी पूर्णांक m ($0 < m < n$ के साथ) के लिए मॉड्यूलर घातांक के साथ हैः

$$(m^e)^d \equiv m (\mathrm{mod}\, n)$$

और यह कि यदि e और n या यहाँ तक कि m भी ज्ञात हो, तो भी d को प्राप्त करना अत्यंत कठिन हो सकता है।

इसके अतिरिक्त, कुछ संक्रियाओं के लिए यह सुविधाजनक है कि दो घातांक के क्रम को बदला जा सकता है और इस संबंध से प्राप्त होता हैः

$$(m^d)^e \equiv m(\text{mod } n)$$

RSA में एक सार्वजनिक कुंजी और एक व्यक्तिगत कुंजी सम्मिलित होती है। सार्वजनिक कुंजी को सभी के द्वारा जाना जा सकता है, और इसका उपयोग संदेशों को एन्क्रिप्ट (कूटित) करने के लिए किया जाता है। आशय यह है कि सार्वजनिक कुंजी के साथ एन्क्रिप्ट (कूटित) किए गए संदेशों को केवल व्यक्तिगत कुंजी का उपयोग करके उचित समय में डिक्रिप्ट (अकूटित) किया जा सकता है। सार्वजनिक कुंजी को पूर्णांक n और e द्वारा दर्शाया गया है; और, पूर्णांक d द्वारा व्यक्तिगत कुंजी, (हालांकि n का उपयोग डिक्रिप्शन (अकूट प्रक्रिया) प्रक्रिया के दौरान भी किया जाता है। इस प्रकार, इसे निजी कुंजी का एक हिस्सा माना जा सकता है)। m संदेश का प्रतिनिधित्व करता है (पहले एक निश्चित तकनीक के साथ तैयार किया गया है जो नीचे समझाया गया है)।

कुंजी का जननः

RSA एल्गोरिथ्म (कलनविधि) के लिए कुंजी निम्नलिखित तरीके से जनित होती हैः

1. दो पृथक–पृथक अभाज्य संख्याएँ p और q चुनें।

सुरक्षा उद्देश्यों के लिए, पूर्णांक p और q को यादृच्छिक रूप से चुना जाना चाहिए, और परिमाण में समान होना चाहिए लेकिन गुणनखण्ड को कठिन बनाने के लिए अंकों की लंबाई भिन्न हो। अभाज्य पूर्णांक कुशलतापूर्वक एक परीक्षण का उपयोग करके पाया जा सकता है। p और q को गुप्त रखा जाता है।

2. $n = pq$ की गणना करें।

n का उपयोग सार्वजनिक और व्यक्तिगत दोनों कुंजियों के लिए मापांक के रूप में किया जाता है। इसकी लंबाई, आम तौर पर बिट्स में व्यक्त की जाती है, यह महत्वपूर्ण लंबाई है। n सार्वजनिक कुंजी के भाग के रूप में जारी किया गया है।

3. $\lambda(n)$ की गणना करें, जहाँ λ Carmichael's टोटिएंट फलन है। चूँकि $n = pq$, $\lambda(n) = \text{lcm}(\lambda(p),\lambda(q))$, और चूँकि p और p अभाज्य हैं, अतः $\lambda(p) = \varphi(p) = p - 1$ और इसी प्रकार $\lambda(q) = q - 1$। इसलिए $\lambda(n) = \text{lcm}(p - 1, q - 1)$। $\lambda(n)$ को गुप्त रखा जाता है।

4. एक पूर्णांक e इस प्रकार चुनें कि $1 < e < \lambda(n)$ और $\gcd(e, \lambda(n)) = 1$; वह है, e और $\lambda(n)$ सहभाज्य हैं।

e एक छोटी बिट–लंबाई और छोटे हैमिंग भार के परिणामस्वरूप अधिक कुशल एन्क्रिप्शन (कूट प्रक्रिया) है – e के लिए सबसे अधिक चुना गया मान $2^{16} + 1 = 5{,}537$ है। e के लिए सबसे छोटा (और सबसे तेज) संभव मान 3 है, लेकिन e के लिए इस तरह के एक छोटे से मान को कुछ परिस्थिति में कम सुरक्षित दिखाया गया है। e सार्वजनिक कुंजी के भाग के रूप में जारी किया गया है।

5. $d \equiv e^{-1} (\text{mod } \lambda(n))$ के रूप में d का निर्धारण करें, अर्थात् d, e modulo $\lambda(n)$ का मॉड्यूलर गुणक व्युत्क्रम है। इसका अर्थ है कि d के लिए समीकरण $d{\cdot}e \equiv 1 (\text{mod } \lambda(n))$ को हल करें। d को विस्तारित यूक्लिडियन एल्गोरिथ्म (कलनविधि) का उपयोग करके कुशलता से गणना की जा सकती है। d को व्यक्तिगत कुंजी घातांक के रूप में गुप्त रखा जाता है।

सार्वजनिक कुंजी मापांक n और सार्वजनिक (या एन्क्रिप्शन) घातांक e रखता है। व्यक्तिगत कुंजी में व्यक्तिगत (या डिक्रिप्शन) घातांक d होता है, जिसे गुप्त रखा जाना चाहिए। p, q और $\lambda(n)$ को भी गुप्त रखना चाहिए क्योंकि इनका उपयोग d की गणना के लिए किया जा सकता है। वास्तव में, उन सभी को d गणना के बाद छोड़ दिया जा सकता है।

मूल RSA शोध–पत्र में, यूलर टोटिएंट फलन यूलर $\varphi(n) = (p - 1)(q - 1)$ का उपयोग व्यक्तिगत घातांक d की गणना के लिए $\lambda(n)$ के स्थान पर किया जाता है। चूँकि $\varphi(n)$ सदैव $\lambda(n)$ द्वारा विभाज्य होता है, एल्गोरिथम (कलनविधि) अच्छा काम करता है। यूलर टोटिएंट फलन का उपयोग किया जा सकता है, इसे लैग्रेंज प्रमेय के परिणाम के रूप में भी देखा जा सकता है जो पूर्णांकों के गुणक समूह मॉडुलो pq पर लागू होता है।

इस प्रकार कोई भी d जो $d{\cdot}e \equiv 1 (\text{mod } \varphi(n))$ को संतुष्ट करता है $d{\cdot}e \equiv 1 (\text{mod } \lambda(n))$ को भी संतुष्ट करेगा। हालांकि, d modulo $\varphi(n)$ की गणना करने से कभी–कभी ऐसा परिणाम निकलेगा जो आवश्यकता से बड़ा हो (अर्थात् $d > \lambda(n)$)।

चूंकि $(p-1)$ और $(q-1)$ के किसी भी सामान्य गुणज के लिए $n-1 = pq-1 = (p-1)(q-1)+(p-1)+(q-1)$ के गुणनखंड में मौजूद हैं। 1), अतः, यह अनुशंसा की जाती है कि $(p-1)$ और $(q-1)$ में केवल बहुत छोटे सामान्य गुणज हैं, यदि आवश्यक 2 के अलावा कोई भी।

कुंजी वितरणः

माना प्रेषक, प्राप्तकर्त्ता को जानकारी भेजना चाहता है। यदि वे RSA का उपयोग करने का निर्णय लेते हैं, तो प्रेषक को संदेश को एन्क्रिप्ट (कूटित) करने के लिए प्राप्तकर्त्ता की सार्वजनिक कुंजी को जानना चाहिए और संदेश को डिक्रिप्ट (कूटित) करने के लिए प्राप्तकर्त्ता को अपनी व्यक्तिगत कुंजी का उपयोग करना चाहिए।

अपने एन्क्रिप्टेड (कूटित) संदेशों को भेजने के लिए प्रेषक को सक्षम करने के लिए, प्राप्तकर्त्ता एक विश्वसनीय, लेकिन जरूरी नहीं कि गुप्त, मार्ग के माध्यम से प्रेषक को अपनी सार्वजनिक कुंजी (n, e) पहुंचाता है। प्राप्तकर्त्ता की व्यक्तिगत कुंजी (d) कभी वितरित नहीं होती है।

एन्क्रिप्शन (कूट प्रक्रिया):

प्रेषक द्वारा प्राप्तकर्त्ता की सार्वजनिक कुंजी प्राप्त करने के बाद, वह प्राप्तकर्त्ता को एक संदेश M भेज सकता है। ऐसा करने के लिए, वह पहले M (नॉन–पैडेड प्लेन–टेक्स्ट) को पूर्णांक m (पैडेड प्लेन–टेक्स्ट) में बदल देता है, इस प्रकार कि सहमत–प्रतिवर्ती प्रोटोकॉल का उपयोग करके जिसे पैडिंग के रूप में जाना जाता है $0 \le m < n$ हो। इसके बाद वह

$$c \equiv m^e (\mathrm{mod}\ n)$$

के संगत प्राप्तकर्त्ता के सार्वजनिक कुंजी e का उपयोग करते हुए, सिफर–टेक्स्ट (कूटलेखन) c की गणना करता है। यह बहुत तेजी से, यहाँ तक कि बहुत बड़ी संख्या के लिए, मॉड्यूलर घातांक का उपयोग करके किया जा सकता है। प्रेषक तब प्राप्तकर्त्ता को c पहुँचाता है।

डिक्रिप्शन (अकूट प्रक्रिया):

प्राप्तकर्त्ता अपनी व्यक्तिगत कुंजी घातांक d का उपयोग कर निम्न गणना द्वारा

$$c^d \equiv (m^e)^d \equiv m (\mathrm{mod}\ n)$$

c से m को पुनर्प्राप्त कर सकता है। m को देखते हुए, वह व्युत्क्रम पैडिंग योजना का उपयोग कर मूल संदेश M को पुनर्प्राप्त कर सकता है।

उदाहरणः

प्राप्तकर्त्ता दो अभाज्य संख्याओं $p = 11$ और $q = 13$ का चयन करके अपनी RSA कुंजियाँ बनाता है। $n = p \times q = 143$ मापांक है। $\phi(n) = (p-1) \times (q-1) = 120$ टोटिएंट फलन है। प्राप्तकर्त्ता अपने RSA सार्वजनिक कुंजी e के लिए 7 चुनता है और विस्तारित यूक्लिडियन एल्गोरिथ्म (कलनविधि) का उपयोग करके RSA व्यक्तिगत कुंजी की गणना करता है, जो उसे 103 देता है।

प्रेषक, प्राप्तकर्त्ता को एक एन्क्रिप्टेड (कूटित) संदेश M भेजना चाहता है, इसलिए वह अपनी RSA सार्वजनिक कुंजी (n, e) प्राप्त करता है, जो इस उदाहरण में (143, 7) है। प्लेन–टेक्स्ट (साधारण–पाठ) संदेश एक संख्या 9 है और इसे सिफर–टेक्स्ट c में निम्न प्रकार एन्क्रिप्ट (कूटित) किया गया हैः

$$M^e \bmod n = 9^7 \bmod 143 = 48 = c$$

जब प्राप्तकर्त्ता को प्रेषक का संदेश मिलता है, तो वह अपनी RSA व्यक्तिगत कुंजी (d, n) का उपयोग करके इस संदेश को निम्न प्रकार डिक्रिप्ट (अकूटित) करता हैः

$$c^d \bmod n = 48^{103} \bmod 143 = 9 = M$$

RSA विश्लेषणः

RSA की सुरक्षा दो अलग–अलग कार्यों की ताकत पर निर्भर करती है। RSA क्रिप्टोसिस्टम सबसे लोकप्रिय सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) है, जो बहुत बड़ी संख्या को गुणनखण्ड करने की व्यावहारिक कठिनाई पर आधारित है।

एन्क्रिप्शन (कूट प्रक्रिया) फलनः इसे प्लेन–टेक्स्ट (साधारण–पाठ) को सिफर–टेक्स्ट (कूटलेख–पाठ) में बदलने का एक–तरफा कार्य माना जाता है और इसे केवल व्यक्तिगत कुंजी d के ज्ञान के साथ उत्क्रम किया जा सकता है।

कुंजी जननः एक RSA सार्वजनिक कुंजी से एक व्यक्तिगत कुंजी का निर्धारण करने की कठिनाई मापांक n के गुणक के बराबर है। इस प्रकार एक हमलावर RSA व्यक्तिगत कुंजी का निर्धारण करने के लिए RSA सार्वजनिक कुंजी के ज्ञान का उपयोग नहीं कर सकता है जब तक कि वह गुणक n नहीं कर सकता। यह एक प्रकार से फलन भी है, p और q मानों से मापांक n तक जाना आसान है, लेकिन व्युत्क्रम संभव नहीं है।

यदि इन दोनों कार्यों में से कोई भी एकतरफा साबित नहीं होता है, तो RSA को तोड़ दिया जाएगा। वास्तव में, यदि कुशलता से गुणक के लिए एक तकनीक विकसित की जाती है, तो RSA सुरक्षित नहीं रहेगा।

आरएसए एन्क्रिप्शन (कूट प्रक्रिया) की ताकत काफी हद तक हमलों के खिलाफ जाती है यदि संख्या p और q बड़े अभाज्य नहीं हैं और/या चुने गए सार्वजनिक कुंजी e एक छोटी संख्या है।

RSA एल्गोरिथ्म (कलनविधि) के लिए C प्रोग्रामः

```
#include<stdio.h>
#include<conio.h>
#include<stdlib.h>
#include<math.h>
#include<string.h>
long int p,q,n,t,flag,e[100],d[100],temp[100],j,m[100],en[100],i;
char msg[100];
int prime(long int);
void ce();
long int cd(long int);
void encrypt();
void decrypt();
void main() {
	clrscr();
	printf("\nENTER FIRST PRIME NUMBER\n");
	scanf("%d",&p);
	flag=prime(p);
	if(flag==0) {
		printf("\nWRONG INPUT\n");
		getch();
		exit(1);
	}
	printf("\nENTER ANOTHER PRIME NUMBER\n");
	scanf("%d",&q);
	flag=prime(q);
	if(flag==0||p==q) {
		printf("\nWRONG INPUT\n");
		getch();
		exit(1);
	}
```

```
        printf("\nENTER MESSAGE\n");
        fflush(stdin);
        scanf("%s",msg);
        for (i=0;msg[i]!=NULL;i++)
        m[i]=msg[i];
        n=p*q;
        t=(p-1)*(q-1);
        ce();
        printf("\nPOSSIBLE VALUES OF e AND d ARE\n");
        for (i=0;i<j-1;i++)
        printf("\n%ld\t%ld",e[i],d[i]);
        encrypt();
        decrypt();
        getch();
}
int prime(long int pr) {
        int i;
        j=sqrt(pr);
        for (i=2;i<=j;i++) {
                if(pr%i==0)
                   return 0;
        }
        return 1;
}
void ce() {
        int k;
        k=0;
        for (i=2;i<t;i++) {
                if(t%i==0)
                   continue;
                flag=prime(i);
                if(flag==1&&i!=p&&i!=q) {
                        e[k]=i;
                        flag=cd(e[k]);
                        if(flag>0) {
                                d[k]=flag;
                                k++;
                        }
                        if(k==99)
                              break;
                }
        }
}
long int cd(long int x) {
        long int k=1;
        while(1) {
```

```
                k=k+t;
                if(k%x==0)
                    return(k/x);
        }
}
void encrypt() {
        long int pt,ct,key=e[0],k,len;
        i=0;
        len=strlen(msg);
        while(i!=len) {
                pt=m[i];

                pt=pt-96;
                k=1;
                for (j=0;j<key;j++) {
                        k=k*pt;
                        k=k%n;
                }
                temp[i]=k;
                ct=k+96;
                en[i]=ct;
                i++;
        }
        en[i]=-1;
        printf("\nTHE ENCRYPTED MESSAGE IS\n");
        for (i=0;en[i]!=-1;i++)
        printf("%c",en[i]);
}
void decrypt() {
        long int pt,ct,key=d[0],k;
        i=0;
        while(en[i]!=-1) {
                ct=temp[i];
                k=1;
                for (j=0;j<key;j++) {
                        k=k*ct;
                        k=k%n;
                }
                pt=k+96;
                m[i]=pt;
                i++;
        }
        m[i]=-1;
        printf("\nTHE DECRYPTED MESSAGE IS\n");
        for (i=0;m[i]!=-1;i++)
        printf("%c",m[i]);
```

}

Output:

```
ENTER FIRST PRIME NUMBER
7
ENTER ANOTHER PRIME NUMBER
17
ENTER MESSAGE
hello
POSSIBLE VALUES OF e AND d ARE
5     77
11    35
13    37
19    91
23    71
29    53
31    31
37    13
THE ENCRYPTED MESSAGE IS
ï △ ccä
THE DECRYPTED MESSAGE IS
hello
```

5.3 ElGamal क्रिप्टोसिस्टम (कूटप्रणाली):

क्रिप्टोग्राफी (कूटलेखन) में, ElGamal एन्क्रिप्शन (कूट प्रक्रिया) प्रणाली सार्वजनिक–कुंजी क्रिप्टोग्राफी (कूटलेखन) के लिए एक असममित कुंजी एन्क्रिप्शन (कूट प्रक्रिया) एल्गोरिथ्मि (कलनविधि) है जो डिफि–हेलमैन कुंजी विनिमय पर आधारित है। यह 1985 में ताहेर एल्गमल द्वारा वर्णित किया गया था। ElGamal एन्क्रिप्शन का उपयोग मुफ्त जीएनयू प्राइवेसी गार्ड सॉफ्टवेयर, पीजीपी के हाल के संस्करणों और अन्य क्रिप्टोसिस्टम (कूटप्रणाली) में किया जाता है। डिजिटल सिग्नेचर एलगोरिथ्मि (अंकीय हस्ताक्षर कलनविधि) ElGamal हस्ताक्षर योजना का एक प्रकार है, जिसे ElGamal एन्क्रिप्शन (कूट प्रक्रिया) के साथ भ्रमित नहीं किया जाना चाहिए।

ElGamal एन्क्रिप्शन (कूट प्रक्रिया) को किसी भी चक्रीय समूह G पर परिभाषित किया जा सकता है, जैसे कि पूर्णांक मॉडुलो n का गुणक समूह। इसकी सुरक्षा कंप्यूटिंग असतत लघुगणक से संबंधित G में एक निश्चित समस्या की कठिनाई पर निर्भर करती है।

RSA के साथ, अन्य सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) प्रस्तावित हैं। उनमें से कई असतत लघुगणक समस्या के विभिन्न संस्करणों पर आधारित हैं।

ElGamal क्रिप्टोसिस्टम (कूटप्रणाली), जिसे एलिप्टिक वक्र विचर (Elliptic Curve Variant) कहा जाता है, असतत लघुगणक समस्या पर आधारित है। यह इस धारणा से ताकत प्राप्त करता है कि असतत लघुगणक किसी दिए गए संख्या के लिए व्यावहारिक समय सीमा में नहीं मिल सकता है, जबकि घात के व्युत्क्रम संक्रिया की कुशलता से गणना की जा सकती है।

अब हम ElGamal के एक सरल संस्करण पर विचार करते हैं जो संख्याओं के मॉडुलो p के साथ काम करता है। दीर्घवृत्तीय वक्र विचर की दशा में, यह विभिन्न संख्या प्रणालियों पर आधारित है।

ElGamal क्रिप्टोसिस्टम (कूटप्रणाली) की योजनाः

माना X, Y से संवाद करना चाहता है।

1. X सार्वजनिक और व्यक्तिगत कुंजी बनाता हैः

- X एक बहुत बड़ी संख्या q और एक चक्रीय समूह F_q चुनता है।
- चक्रीय समूह F_q से, वह किसी भी अवयव g और एक अवयव a को इस प्रकार चुनता है कि gcd(a, q) = 1।
- तब वह $h = g^a$ की गणना करता है।
- X F, $h = g^a$, q और g को अपनी सार्वजनिक कुंजी के रूप में प्रकाशित करता है और a को व्यक्तिगत कुंजी के रूप में रखता है।

2. Y, X की सार्वजनिक कुंजी का उपयोग कर डेटा एन्क्रिप्ट (कूटित) करता है:
   - Y चक्रीय समूह F से एक अवयव k का चयन इस प्रकार करता है कि gcd(k, q) = 1।
   - फिर वह $p = g^k$ और $s = h^k = g^{ak}$ की गणना करता है।
   - वह s को M के साथ गुणा करता है।
   - फिर वह $(p, M*s) = (g^k, M*s)$ भेजता है।
3. X संदेश को डिक्रिप्ट (अकूटित) करता है:
   - X $s' = p^a = g^{ak}$ की गणना करता है।
   - वह M को $s = s'$ के रूप में प्राप्त करने के लिए M*s को s' से विभाजित करता है।

अब हम उपरोक्त एल्गोरिथ्म (कलनविधि) को विस्तार से देखते हैं:

ElGamal कुंजी युग्म का जनन:

ElGamal क्रिप्टोसिस्टम (कूटप्रणाली) का प्रत्येक उपयोगकर्ता निम्न प्रकार कुंजी युग्म बनाता है –

एक बड़ी अभाज्य संख्या p का चयन करना

आम तौर पर 1024 से 2048 बिट्स लंबाई की एक अभाज्य संख्या को चुना जाता है।

एक जनक अवयव g का चयन करना

- यह संख्या 1 और $p - 1$ के मध्य होनी चाहिए, लेकिन कोई भी संख्या नहीं हो सकती है।
- यह पूर्णांक मॉडुलो p के गुणक समूह का एक जनक है। इसका अर्थ है कि प्रत्येक पूर्णांक m के लिए जो p का सह–अभाज्य है, वहाँ एक पूर्णांक k इस प्रकार है कि g^k=a mod n।

  उदाहरण के लिए, 3 समूह 5 ($Z_5 = \{1, 2, 3, 4\}$) का जनक है।

N	3^n	3^n mod 5
1	3	3
2	9	4
3	27	2
4	81	1

व्यक्तिगत कुंजी का चयन:

व्यक्तिगत कुंजी x कोई भी संख्या हो सकती है जो 1 से बड़ी और $p - 1$ से छोटी है।

सार्वजनिक कुंजी के भाग की गणना:

मान y की गणना प्राचल p, g और व्यक्तिगत कुंजी x से निम्नानुसार की जाती है:

$$y = g^x \bmod p$$

सार्वजनिक कुंजी प्राप्त करना:

ElGamal सार्वजनिक कुंजी में तीन प्राचल (p, g, y) होते हैं।

उदाहरण के लिए, माना p = 17 और g = 6 (यह पुष्टि की जा सकती है कि 6 समूह Z_{17} का एक जनक है)। व्यक्तिगत कुंजी x कोई भी संख्या हो सकती है जो 1 से बड़ी हो और 71 से छोटी हो, इसलिए हम x = 5 चुनते हैं। तब y की गणना निम्न प्रकार की जाती है:

$$y = 6^5 \bmod 17 = 7$$

इस प्रकार व्यक्तिगत कुंजी 5 है और सार्वजनिक कुंजी (17, 6, 7) है।

एन्क्रिप्शन (कूट प्रक्रिया) और डिक्रिप्शन (अकूट प्रक्रिया):

RSA के लिए समतुल्य प्रक्रिया की तुलना में ElGamal कुंजी युग्म का जनन तुलनात्मक रूप से सरल है। लेकिन एन्क्रिप्शन (कूट प्रक्रिया) और डिक्रिप्शन (अकूट प्रक्रिया) RSA की तुलना में थोड़ा अधिक जटिल हैं।

ElGamal एन्क्रिप्शन (कूट प्रक्रिया):

माना प्रेषक किसी ऐसे व्यक्ति को एक प्लेन–टेक्स्ट (साधारण–पाठ) भेजना चाहता है, जिसकी ElGamal सार्वजनिक कुंजी (p, g, y) है, तो –

- प्रेषक मॉडुलो p संख्याओं की एक श्रृंखला के रूप में प्लेन–टेक्स्ट (साधारण–पाठ) का प्रतिनिधित्व करता है।
- प्लेन–टेक्स्ट (साधारण–पाठ) P को एन्क्रिप्ट (कूटित) करने के लिए, जिसे एक संख्या मॉडुलो p के रूप में दर्शाया गया है। सिफर–टेक्स्ट (कूटलेख–पाठ) C प्राप्त करने के लिए एन्क्रिप्शन (कूट प्रक्रिया) निम्नानुसार है –
  - यादृच्छिक रूप से एक संख्या k जनित करें।
  - दो मान C1 और C2 की गणना करें, जहाँ –
    $C1 = g^k \bmod p$
    $C2 = (P^* y^k) \bmod p$
- दो अलग–अलग मानों (C1, C2) से मिलकर बने सिफर–टेक्स्ट (कूटलेख–पाठ) C को एक साथ भेजे।
- ऊपर दिए गए ElGamal कुंजी जनन के उदाहरण का उल्लेख करते हुए, प्लेन–टेक्स्ट (साधारण–पाठ) P = 13 को निम्नानुसार एन्क्रिप्ट (कूटित) किया जाता है –
  - यादृच्छिक रूप से एक संख्या k = 10 जनित करें।
  - दो मानों C1 और C2 की गणना करें, जहाँ –
    $C1 = 6^{10} \bmod 17$
    $C2 = (13^* 7^{10}) \bmod 17 = 9$
- सिफरटेक्स्ट (कूटलेख–पाठ) C = (C1, C2) = (15, 9) भेजें।

ElGamal डिक्रिप्शन (अकूट प्रक्रिया):

- व्यक्तिगत कुंजी x का उपयोग करके सिफर–टेक्स्ट (कूटलेख–पाठ) (C1, C2) को डिक्रिप्ट (अकूटित) करने के लिए, निम्नलिखित दो चरणों का पालन किया जाता है:
  - $(C1)^x$ modulo p के मॉड्यूलर व्युत्क्रम की गणना करें, जो $(C1)^{-x}$ है, जिसे आम तौर पर डिक्रिप्शन (अकूट प्रक्रिया) गुणक के रूप में जाना जाता है।
  - निम्नलिखित सूत्र का उपयोग करके प्लेन–टेक्स्ट (साधारण–पाठ) को प्राप्त करें –
    $$C2 \times (C1)^{-x} \bmod p = \text{Plaintext}$$
- उपरोक्त उदाहरण में, व्यक्तिगत कुंजी x = 5 का उपयोग करके सिफर–टेक्स्ट (कूटलेख–पाठ) C = (C1, C2) = (15, 9) को डिक्रिप्ट (अकूटित) करें, डिक्रिप्शन (अकूट प्रक्रिया) गुणक है:
  $15^{-5} \bmod 17 = 9$
- प्लेनटेक्स्ट (साधारण–पाठ) P = (9 × 9) mod 17 = 13 को प्राप्त करें।

ElGamal विश्लेषण:

ElGamal प्रणाली में, प्रत्येक उपयोगकर्ता के पास एक व्यक्तिगत कुंजी x है। और सार्वजनिक कुंजी के तीन घटक हैं – अभाज्य मापांक p, जनक g, और सार्वजनिक $y = g^x \bmod p$। ElGamal की ताकत असतत लघुगणक समस्या की कठिनाई पर आधारित है।

सुरक्षित कुंजी का आकार आम तौर पर 1024 बिट्स से बड़ा होता है। आज भी 2048 बिट्स लंबी कुंजी का उपयोग किया जाता है। प्रसंस्करण गति के मोर्चे पर, ElGamal काफी धीमा है, इसका उपयोग मुख्य रूप से मुख्य प्रमाणीकरण प्रोटोकॉल (संदेशाचार) के लिए किया जाता है। उच्च प्रसंस्करण दक्षता के कारण, ElGamal के एलिप्टिक वक्र विचर तेजी से लोकप्रिय हो रहे हैं।

ElGamal एल्गोरिथ्म (कलनविधि) के लिए C प्रोग्राम:

```
#include <stdio.h>
#include <stdlib.h>
#include <ctype.h>
#include <math.h>
int e1, e2;
int p, d;
int C1, C2;
FILE *out1, *out2;
int gcd(int a, int b)
{
	int q, r1, r2, r;
	if (a > b) {
		r1 = a;
		r2 = b;
	}
	else {
		r1 = b;
		r2 = a;
	}
	while (r2 > 0) {
		q = r1 / r2;
		r = r1 - q * r2;
		r1 = r2;
		r2 = r;
	}
	return r1;
}
int PrimarityTest(int a, int i)
{
	int n = i - 1;
	int k = 0;
	int m, T;

	while (n % 2 == 0) {
		k++;
		n = n / 2;
	}
	m = n;
	T = FindT(a, m, i);
	if (T == 1 || T == i - 1)
		return 1;
	for (int j = 0; j < k; j++) {
		T = FindT(T, 2, i);
		if (T == 1)
			return 0;
```

```
            if (T == i - 1)
                return 1;
        }
        return 0;
}
int PrimitiveRoot(int p)
{
        int flag;
        for (int a = 2; a < p; a++)
        {
            flag = 1;
            for (int i = 1; i < p; i++) {
                if (FindT(a, i, p) == 1 && i < p - 1) {
                    flag = 0;
                }
                else if (flag && FindT(a, i, p) == 1 && i == p - 1) {
                    return a;
                }
            }
        }
}
int KeyGeneration()
{
        do {
            do
                p = rand() + 256;
            while (p % 2 == 0);
        } while (!PrimarityTest(2, p));
        p = 107;
        e1 = 2;
        do {
            d = rand() % (p - 2) + 1; // 1 <= d <= p-2
        } while (gcd(d, p) != 1);

        d = 67;
        e2 = FindT(e1, d, p);
}
int FindT(int a, int m, int n)
{
        int r;
        int y = 1;
        while (m > 0)
        {
            r = m % 2;
            FastExponention(r, n, &y, &a);
```

```
                m = m / 2;
        }
        return y;
}
int FastExponention(int bit, int n, int* y, int* a)
{
        if (bit == 1)
                *y = (*y * (*a)) % n;

        *a = (*a) * (*a) % n;
}
int Encryption(int Plaintext)
{
        out1 = fopen("cipher1.txt", "a+");
        out2 = fopen("cipher2.txt", "a+");
        int r;
        do {
                r = rand() % (p - 1) + 1; // 1 < r < p
        }
        while (gcd(r, p) != 1);

        C1 = FindT(e1, r, p);
        C2 = FindT(e2, r, p) * Plaintext % p;
        fprintf(out1, "%d ", C1);
        fprintf(out2, "%d ", C2);
        fclose(out1);
        fclose(out2);
}
int Decryption(int C1, int C2)
{
        FILE* out = fopen("result.txt", "a+");
        int decipher = C2 * FindT(C1, p - 1 - d, p) % p;
        fprintf(out, "%c", decipher);
        fclose(out);
}
int main()
{
        FILE *out, *inp;
        // destroy contents of these files (from previous runs, if any)
        out = fopen("result.txt", "w+");
        fclose(out);
        out = fopen("cipher1.txt", "w+");
        fclose(out);
        out = fopen("cipher2.txt", "w+");
        fclose(out);
        KeyGeneration();
```

```
        inp = fopen("plain.txt", "r+");
        if (inp == NULL) {
                printf("Error opening Source File.\n");
                exit(1);
        }
        while (1)
        {
                char ch = getc(inp);
                if (ch == EOF)
                        break;  // M < p
                Encryption(toascii(ch));
        }
        fclose(inp);
        fclose(out);
        FILE *inp1, *inp2;
        inp1 = fopen("cipher1.txt", "r");
        inp2 = fopen("cipher2.txt", "r");
        int C1, C2;
        while (1)
        {
                int ret = fscanf(inp1, "%d", &C1);
                fscanf(inp2, "%d", &C2);
                if (ret == -1)
                        break;
                Decryption(C1, C2);
        }
        fclose(inp1);
        fclose(inp2);
        return 0;
}
```

5.4 एलिप्टिक–वक्र क्रिप्टोग्राफी (अण्डाकार–वक्र कूटलेखन) (ECC):

एलिप्टिक–वक्र क्रिप्टोग्राफी (अण्डाकार–वक्र कूटलेखन) परिमित क्षेत्रों पर दीर्घवृत्तीय वक्रों की बीजगणितीय संरचना के आधार पर सार्वजनिक–कुंजी क्रिप्टोग्राफी (कूटलेखन) के लिए एक दृष्टिकोण है। समतुल्य सुरक्षा प्रदान करने के लिए ECC को अ–एलिप्टिक–वक्र क्रिप्टोग्राफी (कूटलेखन) की तुलना में छोटी कुंजी की आवश्यकता होती है।

एलिप्टिक–वक्र (अण्डाकार–वक्र, डिजिटल (अंकीय) हस्ताक्षर, छद्म यादृच्छिक जनक और अन्य कार्यों के लिए लागू होते हैं। अप्रत्यक्ष रूप से, उन्हें एक सममित एन्क्रिप्शन (कूट प्रक्रिया) योजना के साथ कुजी समझौते को जोड़कर एन्क्रिप्शन (कूट प्रक्रिया) के लिए उपयोग किया जा सकता है। वे कई पूर्णांक गुणनखण्ड एल्गोरिथ्म (कलनविधि) में भी उपयोग किए जाते हैं जो कि एलिप्टिक वक्रों पर आधारित होते हैं, जिनमें क्रिप्टोग्राफी (कूटलेखन) में अनुप्रयोग होते हैं, जैसे कि लेनस्ट्रा एलिप्टिक–वक्र गुणन।

सार्वजनिक–कुंजी क्रिप्टोग्राफी (कूटलेखन) कुछ गणितीय समस्याओं की सहजता पर आधारित है। प्रारंभिक सार्वजनिक–कुंजी प्रणाली यह मानकर सुरक्षित हैं कि दो या दो से अधिक बड़े प्रमुख गुणकों से बने एक बड़े पूर्णांक को बनाना मुश्किल है। एलिप्टिक–वक्र–आधारित प्रोटोकॉल (संदेशाचार) के लिए, यह माना जाता है कि एक सार्वजनिक रूप से ज्ञात आधार बिंदु के संबंध में एक यादृच्छिक एलिप्टिक वक्र अवयव के असतत लघुगणक को खोजना संभव हैः यह एलिप्टिक वक्र असतत लघुगणक समस्या है।

एलिप्टिक वक्र क्रिप्टोग्राफी (कूटलेखन) की सुरक्षा एक बिंदु गुणन की गणना करने की क्षमता और मूल उत्पाद बिंदुओं को देखते हुए गुणक की गणना करने में असमर्थता पर निर्भर करती है। एलिप्टिक वक्र का आकार समस्या की कठिनाई को निर्धारित करता है।

एलिप्टिक वक्र क्रिप्टोग्राफी (कूटलेखन) द्वारा आश्वस्त किया गया प्राथमिक लाभ एक छोटा कुंजी आकार है, जो भंडारण और संचरण आवश्यकताओं को कम करता है, अर्थात् कि एक एलिप्टिक वक्र समूह एक बड़े मापांक के साथ RSA आधारित प्रणाली द्वारा की गई सुरक्षा के समान स्तर प्रदान कर सकता है और इसी प्रकार बड़ी कुंजी के लिए भी। उदाहरण के लिए, एक 256–बिट एलिप्टिक वक्र सार्वजनिक कुंजी को 3072–बिट RSA सार्वजनिक कुंजी के लिए तुलनीय सुरक्षा प्रदान करनी चाहिए।

एलिप्टिक वक्र क्रिप्टोग्राफी (कूटलेखन) एक सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) तकनीक है जो एलिप्टिक वक्र सिद्धांत पर आधारित है जिसका उपयोग तेजी से, छोटे और अधिक कुशल क्रिप्टोग्राफिक (कूटलेखीय) कुंजियों को बनाने के लिए किया जा सकता है। ECC बहुत बड़ी अभाज्य संख्याओं के उत्पाद के रूप में पारंपरिक विधि के बजाय एलिप्टिक वक्र समीकरण के गुणों के माध्यम से कुंजी उत्पन्न करता है। प्रौद्योगिकी का उपयोग अधिकांश सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) विधियों जैसे RSA और डिफी–हेलमैन के साथ संयोजन में किया जा सकता है।

कुछ शोधकर्ताओं के अनुसार, ECC 164–बिट कुंजी के साथ सुरक्षा स्तर का उत्पादन कर सकती है जिसे हासिल करने के लिए अन्य प्रणालियों को 1,024–बिट कुंजी की आवश्यकता होती है। क्योंकि ECC कम कंप्यूटिंग शक्ति और बैटरी संसाधन उपयोग के साथ समान सुरक्षा स्थापित करने में मदद करता है, इसलिए इसे मोबाइल अनुप्रयोगों के लिए व्यापक रूप से उपयोग किया जा रहा है। ECC, एक मोबाइल ई–बिजनेस सुरक्षा प्रदाता, सर्टिफिकेशन द्वारा विकसित किया गया था, और हाल ही में एकीकृत सर्किट (IC) और नेटवर्क सुरक्षा उत्पादों के निर्माता द्वारा लाइसेंस प्राप्त किया गया था। RSA ECC का अपना संस्करण विकसित कर रहा है। 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW और VeriFone सहित कई निर्माताओं ने अपने उत्पादों में ECC के लिए समर्थन शामिल किया है।

एलिप्टिक वक्रों के गुणों और कार्यों का गणित में 150 वर्षों तक अध्ययन किया गया है। क्रिप्टोग्राफी के भीतर उनका उपयोग पहली बार 1985 में (पृथक से) वाशिंगटन विश्वविद्यालय से नील कोब्लिट्ज और आईबीएम में विक्टर मिलर द्वारा प्रस्तावित किया गया था। एक एलिप्टिक वक्र एक दीर्घवृत्त (अंडाकार आकृति) नहीं है, लेकिन दो अक्षों (एक बिंदु की स्थिति को इंगित करने के लिए उपयोग किए गए ग्राफ पर रेखाएं) को पार करने वाली एक लूपिंग रेखा के रूप में दर्शाया गया है। ECC गणितीय समूह से बनाए गए एक विशेष प्रकार के समीकरण के गुणों पर आधारित है (मानों का एक समूह जिसके लिए समूह के किसी भी दो सदस्यों पर एक तीसरे सदस्य को उत्पन्न करने के लिए संचालन किया जा सकता है) जो उन बिंदुओं से उत्पन्न होता है जहां रेखा अक्षों को काटती है। एक बिंदु पर वक्र को एक संख्या से गुणा करने से वक्र पर एक और बिंदु उत्पन्न होगा, लेकिन यह पता लगाना बहुत मुश्किल है कि किस संख्या का उपयोग किया गया था, भले ही आपको मूल बिंदु और परिणाम पता हो। एलिप्टिक वक्रों पर आधारित समीकरणों की एक विशेषता है जो क्रिप्टोग्राफी (कूटलेखन) के उद्देश्यों के लिए बहुत मूल्यवान है, वे प्रदर्शन करने में अपेक्षाकृत आसान हैं, और व्युत्क्रम करने के लिए अत्यधिक कठिन हैं।

एलिप्टिक कर्व क्रिप्टोग्राफी (कूटलेखन) एक शब्द है जिसका उपयोग क्रिप्टोग्राफिक (कूटलेखन) उपकरण और प्रोटोकॉल (संदेशाचार) के एक सूट का वर्णन करने के लिए किया जाता है, जिसकी सुरक्षा असतत लघुगणक समस्या के विशेष संस्करणों पर आधारित है। यह संख्या मॉडुलो p का उपयोग नहीं करता है।

ECC उन संख्याओं के सेट पर आधारित है जो गणितीय वस्तुओं से संबंधित हैं जिन्हें दीर्घवृत्तीय वक्र कहा जाता है। इन संख्याओं के गुणकों को जोड़ने और उनकी गणना करने के नियम हैं, ठीक उसी तरह जैसे संख्याओं के लिए मॉडुलो p।

ECC में कई क्रिप्टोग्राफिक (कूटलेखन) योजनाओं का एक विचर सम्मिलित है, जिन्हें आरंभ में ElGamal एन्क्रिप्शन (कूट प्रक्रिया) और डिजिटल सिग्नेचर एल्गोरिथम (कलनविधि) जैसे मॉड्यूलर संख्या के लिए डिजाइन किया गया था।

यह माना जाता है कि एलिप्टिक वक्र पर बिंदुओं पर लागू होने पर असतत लघुगणक समस्या बहुत कठिन है। यह एक एलिप्टिक वक्र पर संख्या मॉडुलो p से बिंदुओं पर स्विच करने का संकेत देता है। यदि हम एलिप्टिक वक्र–आधारित विचर का उपयोग करते हैं, तो भी एक समान सुरक्षा स्तर छोटी कुंजी के साथ प्राप्त किया जा सकता है।

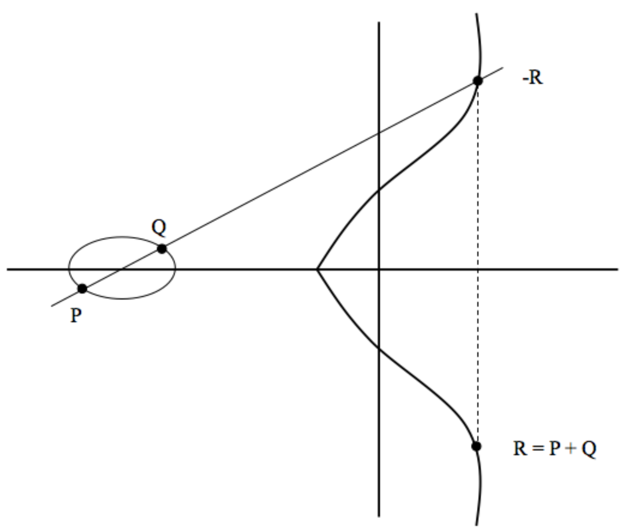
छोटी कुंजी के परिणामस्वरूप दो लाभ होते हैं –

- प्रमुख प्रबंधन में आसानी
- कुशल संगणना

ये लाभ एन्क्रिप्शन (कूट प्रक्रिया) योजना के एलिप्टिक–वक्र–आधारित विचर को अनुप्रयोग के लिए अत्यधिक आकर्षक बनाते हैं जहाँ कंप्यूटिंग संसाधन विवश हैं।

एलिप्टिक वक्र संख्या सिद्धांत और बीजगणितीय ज्यामिति को मिलाते हैं। इन वक्रों को संख्याओं के किसी भी क्षेत्र (अर्थात्, वास्तविक, पूर्णांक, सम्मिश्र) पर परिभाषित किया जा सकता है, हालांकि हम आम तौर पर उन्हें क्रिप्टोग्राफी (कूटलेखन) में अनुप्रयोगों के लिए परिमित क्षेत्रों में उपयोग करते हुए देखते हैं। एक एलिप्टिक वक्र में वास्तविक संख्या (x, y) का समुच्चय होता है जो निम्न समीकरण को संतुष्ट करता है: $y^2 = x^3 + ax + b$

समीकरण के सभी समाधानों का समूह एलिप्टिक वक्र बनाता है। a और b को आपस में बदलने से वक्र का आकार बदल जाता है, और इन मापदंडों में छोटे बदलाव से (x, y) समाधानों के सेट में बड़े बदलाव हो सकते हैं।



(चित्र क्र0 5.2; स्त्रोतः इंटरनेट से साभार)

उपरोक्त चित्र एक एलिप्टिक वक्र पर दो बिंदुओं को जोड़ने को दर्शाता है। एलिप्टिक वक्रों में दिलचस्प गुण है जो एलिप्टिक वक्र पर दो बिंदुओं को जोड़ने से वक्र पर तीसरा बिंदु उत्पन्न होता है। इसलिए, दो बिंदुओं को जोड़कर, P और Q, हमें वक्र पर R को इंगित करता है। P या Q में छोटे परिवर्तन R की स्थिति में बड़े बदलाव का कारण बन सकते हैं।

बिंदु Q की शुरुआत, P या Q = nP के कई बिंदुओं के रूप में की जाती है। एक हमलावर को P और Q पता हो सकता है लेकिन पूर्णांक, n को खोजना, हल करना एक कठिन समस्या है। Q (अर्थात्, nP) सार्वजनिक कुंजी है और n व्यक्तिगत कुंजी है।

चूंकि ECC कुंजी आकार तुलनीय RSA कुंजी की तुलना में बहुत छोटा है, इसलिए सार्वजनिक कुंजी और व्यक्तिगत कुंजी की लंबाई एलिप्टिक वक्र क्रिप्टोसिस्टम्स (कूटप्रणाली) में बहुत कम है।

यह तेजी से प्रसंस्करण समय में परिणाम है, और मेमोरी तथा बैंडविड्थ पर कम मांग, कुछ अध्ययनों में पाया गया है कि हस्ताक्षर और डिक्रिप्शन (अकूट प्रक्रिया) के लिए ECC, RSA से तीव्र है, लेकिन हस्ताक्षर सत्यापन और एन्क्रिप्शन (कूट प्रक्रिया) के लिए धीमी है।

सामान्य तौर पर दिखने वाला एक एलिप्टिक वक्र नीचे चित्र में दिखाया गया है। जब एक सीधी रेखा वक्र को काटती है तो एलिप्टिक वक्र अधिकतम 3 बिंदुओं को काट सकते हैं। जैसा कि हम देख सकते हैं कि एलिप्टिक वक्र x-अक्ष के परितः सममित है, यह गुण एल्गोरिथम (कलनविधि) में एक महत्वपूर्ण भूमिका निभाता है।

इस विधि में छः टपल्स {P, a, b, G, n, h} का उपयोग किया जाता है। जहाँ

P = वह क्षेत्र जहाँ वक्र परिभाषित है, G = जनक बिन्दु

a, b = वक्र पर परिभाषित मान

h = सह–गुणक

n = G का अभाज्य क्रम

डिफी–हेलमैन एल्गोरिथ्म (कलनविधि) का उपयोग एक साझा रहस्य को स्थापित करने के लिए किया जाता है जिसका उपयोग गुप्त संचार के लिए किया जा सकता है जबकि अंक उत्पन्न करने और मापदंडों का उपयोग करके गुप्त कुंजी प्राप्त करने के लिए एलिप्टिक वक्र का उपयोग करके एक सार्वजनिक नेटवर्क पर डेटा का आदान–प्रदान किया जाता है।

एल्गोरिथ्म (कलनविधि) की सादगी और व्यावहारिक कार्यान्वयन के लिए, हम केवल 4 चर एक अभाज्य P और G (P का पूर्वग मूल) और दो व्यक्तिगत मानों a और b पर विचार करेंगे।

P और G दोनों सार्वजनिक रूप से उपलब्ध संख्या हैं। उपयोगकर्ता व्यक्तिगत मानों को a और b चुनते हैं और वे एक कुंजी उत्पन्न करते हैं और इसे सार्वजनिक रूप से विनिमय करते हैं, दूसरे व्यक्ति को कुंजी प्राप्त होती है और उसी से एक गुप्त कुंजी उत्पन्न होती है जिसके बाद उनके पास एन्क्रिप्ट करने के लिए एक ही गुप्त कुंजी होती है।

X	Y
उपलब्ध सार्वजनिक कुंजी = P, G	उपलब्ध सार्वजनिक कुंजी = P, G
चयनित व्यक्तिगत कुंजी = a	चयनित व्यक्तिगत कुंजी = b
जनित कुंजी = $x = G^a \mod P$	जनित कुंजी = $y = G^b \mod P$
जनित कुंजी को आपस में बदलना	
प्राप्त कुजी = y	प्राप्त कुजी = x
गुप्त कुंजी का जनन = $K_a = y^a \mod P$	गुप्त कुंजी का जनन = $K_b = x^b \mod P$
बीजगणितीय रूप में इसे $K_a = K_b$ प्रकार से दिखाया जायेगा	

अब उपयोगकर्त्ता के पास एन्क्रिप्ट (कूटित) करने के लिए एक सममित गुप्त कुंजी है।

उदाहरणः

चरण 1: X और Y के पास सार्वजनिक संख्या P = 23, G = 9 है।

चरण 2: X ने एक व्यक्तिगत कुंजी a = 4 का चयन किया और
Y ने एक व्यक्तिगत कुंजी b = 3 का चयन किया

चरण 3: X और Y सार्वजनिक मानों की गणना करते हैं।

X: $x = (9^4 \mod 23) = (6561 \mod 23) = 6$

Y: $y = (9^3 \mod 23) = (729 \mod 23) = 16$

चरण 4: X और Y सार्वजनिक संख्याओं का आदान–प्रदान करते हैं।

चरण 5: X को सार्वजनिक कुंजी y = 16 प्राप्त होती है और
Y को सार्वजनिक कुंजी x = 6 प्राप्त होता है।

चरण 6: X और X सममित कुंजी की गणना करते हैं

X: $ka = y^a \mod p = 65536 \mod 23 = 9$

Y: $kb = x^b \mod p = 216 \mod 23 = 9$

चरण 7: 9 साझा रहस्य है।

5.5 संयोजन तकनीकः सिमेट्रिक और असिमेट्रिक एन्क्रिप्शन (सममित और असममित कूट प्रक्रिया)

सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) का उपयोग करने का नुकसान यह है कि यह एक धीमी प्रक्रिया है क्योंकि कुंजी की लंबाई बड़ी है (1024 बिट्स से 4094 बिट्स)।

जब हम दोनों प्रक्रियाओं की तुलना करते हैं, तो गुप्त कुंजी एन्क्रिप्शन (कूट प्रक्रिया) काफी तेज होता है क्योंकि कुंजी की लंबाई कम होती है (40 बिट्स से 256 बिट्स)। दूसरी ओर, कुंजी को गुप्त कुंजी एन्क्रिप्शन (कूट प्रक्रिया) में स्थानांतरित करने में समस्या है। इन दोनों तकनीकों का उपयोग एन्क्रिप्शन (कूट प्रक्रिया) की बेहतर विधि प्रदान करने के लिए एक साथ किया जा सकता है। इस प्रकार हम संयुक्त लाभ का उपयोग कर सकते हैं और नुकसान को दूर कर सकते हैं।

एक संयुक्त तकनीक में डेटा स्थानांतरण के चरण हैं:

1. एक सममित एन्क्रिप्शन (कूट प्रक्रिया) का उपयोग करके अपनी फाइल को एन्क्रिप्ट (कूटित) करें।
2. प्राप्तकर्ता की सार्वजनिक कुंजी का उपयोग करके केवल इस कुंजी को एन्क्रिप्ट (कूटित) करने के लिए असममित एन्क्रिप्शन (कूट प्रक्रिया) का उपयोग करें। अब प्राप्तकर्ता को एन्क्रिप्टेड (कूटित) कुंजी भेजें। प्राप्तकर्ता, अंत में, अब अपनी निजी कुंजी का उपयोग करके कुंजी को डिक्रिप्ट (अकूटित) कर सकता है।
3. इसके उपरांत, वास्तविक एन्क्रिप्टेड (कूटित) डेटा भेजें। एन्क्रिप्टेड (कूटित) डेटा को उस कुंजी का उपयोग करके डिक्रिप्ट (अकूटित) किया जा सकता है जिसे असममित कुंजी जोड़ी से सार्वजनिक कुंजी का उपयोग करके एन्क्रिप्ट (कूटित) किया गया था।

एन्क्रिप्शन (कूट प्रक्रिया) की संयुक्त तकनीक व्यापक रूप से उपयोग की जाती है। यह मूल रूप से सुरक्षित शेल (SSH) के लिए उपयोग किया जाता है, जिसका उपयोग क्लाइंट और सर्वर के बीच संचार को सुरक्षित रखने और संदेश भेजने के लिए PGP के लिए किया जाता है। इन सबसे ऊपर, यह सुरक्षित सॉकेट्स परत (SSL) का दिल है, जो एक दूसरे के साथ सुरक्षित संचार चैनल को बनाए रखने के लिए वेब ब्राउजर और वेब सर्वर द्वारा व्यापक रूप से उपयोग किया जाता है।

एक प्रणाली से दूसरे नेटवर्क पर सार्वजनिक नेटवर्क द्वारा स्थानांतरित किए गए डेटा को एन्क्रिप्शन (कूट प्रक्रिया) की विधि द्वारा संरक्षित किया जा सकता है। एन्क्रिप्शन (कूट प्रक्रिया) पर डेटा को 'कुंजी' का उपयोग करके किसी भी एन्क्रिप्शन (कूट प्रक्रिया) एल्गोरिथ्म (कलनविधि) द्वारा एन्क्रिप्ट/स्क्रैम्बल (कूटित) किया जाता है। केवल उसी कुंजी की पहुँच रखने वाले उपयोगकर्ता एन्क्रिप्ट (कूटित) किए गए डेटा को डीक्रिप्ट/डी–स्क्रैम्बल (अकूटित) कर सकते हैं।

इस विधि को व्यक्तिगत कुंजी या सममित कुंजी क्रिप्टोग्राफी (कूटलेखन) के रूप में जाना जाता है। कई मानक सममित कुंजी एल्गोरिथ्म (कलनविधि) परिभाषित हैं। उदाहरण AES, 3DES आदि। इन मानक सममित एल्गोरिथ्म (कलनविधि) को परिभाषित किया गया है जो अत्यधिक सुरक्षित और समय पर परीक्षण किए गए साबित होते हैं। लेकिन इन एल्गोरिथ्म (कलनविधि) के साथ समस्या कुंजी विनिमय है।

संचार पक्षों को एक साझा गुप्त कुंजी की आवश्यकता होती है, एक सुरक्षित संचार के लिए उनके बीच आदान–प्रदान किया जाना चाहिए। सममित कुंजी एल्गोरिथ्म (कलनविधि) की सुरक्षा कुंजी की गोपनीयता पर निर्भर करती है। उपयोग किए गए एल्गोरिथ्म के आधार पर कुंजी की लंबाई आमतौर पर सैकड़ों बिट्स की होती है।

चूंकि संचार पक्षों के मध्य मध्यवर्ती बिंदुओं की संख्या हो सकती है, जिसके माध्यम से डेटा गुजरता है, इन कुंजियों को सुरक्षित तरीके से ऑनलाइन एक्सचेंज नहीं किया जा सकता है। एक बड़े नेटवर्क में, जहाँ सैकड़ों सिस्टम जुड़े हुए हैं, ऑफलाइन कुंजी विनिमय बहुत मुश्किल और यहाँ तक कि अवास्तविक लगता है।

यह वह जगह है जहाँ सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) मदद करने के लिए आती है। सार्वजनिक कुंजी एल्गोरिथ्म (कलनविधि) का उपयोग करके किसी भी गुप्त डेटा के आदान–प्रदान की आवश्यकता वाले संचार पक्षों के मध्य एक साझा रहस्य को ऑनलाइन स्थापित किया जा सकता है।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) में प्रत्येक उपयोगकर्ता या संचार में भाग लेने वाले डिवाइस में कुंजियों की एक जोड़ी होती है, एक सार्वजनिक कुंजी और एक व्यक्तिगत कुंजी होती है, और क्रिप्टोग्राफिक (कूटलेखीय) संचालन करने के लिए कुंजी के साथ जुड़े कार्यों का एक समूह होता है।

केवल विशेष उपयोगकर्ता/उपकरण व्यक्तिगत कुंजी जानता है, जबकि सार्वजनिक कुंजी सभी उपयोगकर्ताओं/उपकरणों को संचार में भाग लेने के लिए वितरित की जाती है। चूंकि सार्वजनिक कुंजी का ज्ञान एल्गोरिथ्म (कलनविधि) की सुरक्षा से समझौता नहीं करता है, इसलिए इसे आसानी से ऑनलाइन विनिमय किया जा सकता है।

एक साझा रहस्य को दो संचार पक्षों के मध्य केवल सार्वजनिक कुंजी और सार्वजनिक स्थिरांक का आदान–प्रदान करके ऑनलाइन स्थापित किया जा सकता है। कोई भी तृतीय पक्ष, जिनके पास केवल विनमय की गई सार्वजनिक सूचनाओं तक पहुंच है, वे साझा रहस्य की गणना नहीं कर पाएंगे, जब तक कि किसी भी संवाद करने वाले पक्षों की व्यक्तिगत कुंजी तक पहुँच न हो।

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) में, कुंजी और संदेश संख्यात्मक रूप से व्यक्त किए जाते हैं और संचालन गणितीय रूप से व्यक्त किए जाते हैं। डिवाइस की व्यक्तिगत और सार्वजनिक कुंजी गणितीय कार्य से संबंधित है जिसे एक–पक्षीय फलन कहा जाता है। एक–पक्षीय फलन गणितीय फलन हैं जिनमें अग्र संक्रिया आसानी से किया जा सकता है लेकिन व्युत्क्रम संक्रिया इतना कठिन है कि यह व्यावहारिक रूप से असंभव है। सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) में सार्वजनिक कुंजी की गणना एक पक्षीय फलन के आगे संचालन पर व्यक्तिगत कुंजी का उपयोग करके की जाती है।

सार्वजनिक कुंजी से व्यक्तिगत कुंजी प्राप्त करना एक व्युत्क्रम संक्रिया है। यदि व्युत्क्रम संक्रिया आसानी से किया जा सकता है, अर्थात यदि व्यक्तिगत कुंजी को सार्वजनिक कुंजी और अन्य सार्वजनिक डेटा से प्राप्त किया जाता है, तो विशेष कुंजी के लिए सार्वजनिक कुंजी एल्गोरिथ्म (कलनविधि) को उदभ्रांत किया जाता है। कुंजी आकार बढ़ने पर व्युत्क्रम संक्रिया कठिन हो जाता है। सार्वजनिक कुंजी एल्गोरिथ्म (कलनविधि) व्युत्क्रम संक्रिया को व्यावहारिक रूप से असंभव बनाने के लिए पर्याप्त संख्या में काम करते हैं और इस प्रकार सिस्टम को सुरक्षित बनाते हैं। उदाहरण के लिए, RSA एल्गोरिथ्म (कलनविधि) हजारों बिट्स की बड़ी संख्या पर काम करता है।

क्रिप्टोग्राफी (कूटलेखन) में, एक हाइब्रिड क्रिप्टोसिस्टम (संकर कूटप्रणाली) वह है जो एक सममित–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) की दक्षता के साथ एक सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) की सुविधा को जोड़ता है। सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) सुविधाजनक है कि उन्हें सुरक्षित रूप से (अन्य उपयोगी गुणों के मध्य) संवाद करने के लिए एक सामान्य रहस्य साझा करने के लिए प्रेषक और उपयोगकर्त्ता की आवश्यकता नहीं है। हालांकि, वे अक्सर जटिल गणितीय संगणनाओं पर भरोसा करते हैं और इस प्रकार तुलनीय सममित–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) की तुलना में आम तौर पर बहुत अधिक अक्षम होते हैं। कई अनुप्रयोगों में, सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) में लंबे संदेशों को एन्क्रिप्ट (कूटित) करने की उच्च्य लागत निषेधात्मक हो सकती है। यह दोनों के संयोजन का उपयोग करके हाइब्रिड (संकर) प्रणाली द्वारा संबोधित किया जाता है।

एक हाइब्रिड क्रिप्टोसिस्टम (संकर कूटप्रणाली) का निर्माण किन्हीं भी दो पृथक क्रिप्टोसिस्टम (कूटप्रणाली) के उपयोग से किया जा सकता हैः

- एक कुंजी एन्कैप्सुलेशन योजना, जो एक सार्वजनिक–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) है
- एक डेटा एनकैप्सुलेशन योजना, जो एक सममित–कुंजी क्रिप्टोसिस्टम (कूटप्रणाली) है

हाइब्रिड क्रिप्टोसिस्टम (कूटप्रणाली) अपने आप में एक सार्वजनिक–कुंजी प्रणाली है, जिसकी सार्वजनिक और व्यक्तिगत कुंजी, कुंजी एन्कैप्सुलेशन स्कीम में समान हैं।

स्मरण रहे बहुत लंबे संदेशों के लिए एन्क्रिप्शन/डिक्रिप्शन (कूट/अकूट प्रक्रिया) में कार्य अधिक कुशल सममित–कुंजी योजना द्वारा किया जाता है, जबकि अक्षम सार्वजनिक कुंजी योजना का उपयोग केवल एक छोटे कुंजी मान को एन्क्रिप्ट/डिक्रिप्ट (कूटित/अकूटित) करने के लिए किया जाता है।

X को हाइब्रिड क्रिप्टोसिस्टम (संकर कूटप्रणाली) में दिए गए संदेश को एन्क्रिप्ट (कूटित) करने के लिए, Y निम्नलिखित कार्य करता हैः

1. X की सार्वजनिक कुंजी प्राप्त करता है।
2. डेटा एनकैप्सुलेशन योजना के लिए एक नई सममित कुंजी बनाता है।
3. डेटा एनकैप्सुलेशन स्कीम के तहत मैसेज को एनक्रिप्ट (कूटित) करता है, ठीक उसी समय जनित की गई सममित कुंजी का उपयोग करके।

4. X की सार्वजनिक कुंजी का उपयोग करते हुए, प्रमुख एन्कैप्सुलेशन योजना के तहत सममित कुंजी को एनक्रिप्ट (कूटित) करता है।
5. इन दोनों एनक्रिप्शन (कूट प्रक्रिया) को X के पास भेजता है।

इस हाइब्रिड सिफर–टेक्स्ट (कूटलेख–पाठ) को डिक्रिप्ट (अकूटित) करने के लिए, X निम्नलिखित कार्य करता हैः

1. कुंजी एनकैप्सुलेशन खण्ड में सम्मिलित सममित कुंजी को डिक्रिप्ट (अकूटित) करने के लिए अपनी व्यक्तिगत कुंजी का उपयोग करता है।
2. डेटा इनकैप्सुलेशन खण्ड में निहित संदेश को डिक्रिप्ट (अकूटित) करने के लिए इस सममित कुंजी का उपयोग करता है।

अधिकांश अनुप्रयोगों में, प्रत्येक पद्धति की ताकत का लाभ उठाने के लिए सममित और असममित एन्क्रिप्शन (कूट प्रक्रिया) को संयोजित किया जाता है। जब सममित और असममित एन्क्रिप्शन (कूट प्रक्रिया) को संयोजित किया जाता है, तो निम्न कार्य होता हैः

सममित एन्क्रिप्शन (कूट प्रक्रिया) का उपयोग प्लेन–टेक्स्ट (साधारण–पाठ) को सिफर–टेक्स्ट (कूटलेख–पाठ) में बदलने के लिए किया जाता है। यह सममित एन्क्रिप्शन (कूट प्रक्रिया) गति का लाभ उठाता है।

असममित एन्क्रिप्शन (कूट प्रक्रिया) का उपयोग एन्क्रिप्शन (कूट प्रक्रिया) के लिए उपयोग की जाने वाली सममित कुंजी का आदान–प्रदान करने के लिए किया जाता है। यह असममित एन्क्रिप्शन (कूट प्रक्रिया) की सुरक्षा का लाभ उठाता है, यह सुनिश्चित करता है कि केवल इच्छित प्राप्तकर्ता सममित कुंजी को डिक्रिप्ट (अकूटित) कर सकता है।

अभ्यास

1. पब्लिक की क्रिप्टोग्राफी (सार्वजनिक कुंजी कूटेखन) से क्या समझते हैं?
2. RSA क्रिप्टोसिस्टम (कूटप्रणाली) पर संक्षिप्त टिप्पणी लिखिए।
3. ElGamal क्रिप्टोसिस्टम (कूटप्रणाली) को विस्तार से समझाइए।
4. एलिप्टिक–कर्व क्रिप्टोग्राफी (अण्डाकार–वक्र कूटलेखन) क्या है?
5. सिमेट्रिक और असिमेट्रिक एन्क्रिप्शन (सममित और असममित कूट प्रक्रिया) संयोजन तकनीक को समझाइए।

अध्याय – 6

हैश फंक्शन
(द्रुतान्वेषण फलन)

6.1 क्रिप्टोग्राफी हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन):

क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) एक हैश फंक्शन (द्रुतान्वेषण फलन) है जो क्रिप्टोग्राफी (कूटलेखन) में उपयोग के लिए उपयुक्त है। यह एक गणितीय एल्गोरिथ्म (कलनविधि) है जो एक निश्चित आकार (हैश मान, हैश या मैसेज डाइजेस्ट) के एक बिट स्ट्रिंग के लिए मनमाने आकार (अक्सर संदेश) के डेटा को प्रतिचित्रित करता है और एक–तरफा है, अर्थात्, एक ऐसा फलन जो व्यावहारिक रूप से इनवर्टर के लिए व्युत्क्रम है। आदर्श रूप से, किसी संदेश को खोजने का एकमात्र तरीका जो दिए गए हैश (द्रुतान्वेषण) का उत्पादन करता है, संभावित इनपुट्स (निवेश) की एक क्रूर–बल खोज का प्रयास करता है, ताकि यह देखा जा सके कि वे एक सुमेलन का उत्पादन करते हैं, या मिलान किए गए हैश (द्रुतान्वेषण) के इंद्रधनुष तालिका का उपयोग करते हैं। क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) आधुनिक क्रिप्टोग्राफी (कूटलेखन) का एक मूल उपकरण है।

क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) सूचना सुरक्षा में डेटा की अखंडता, प्रमाणीकरण नियंत्रण और अन्य सुरक्षा तंत्र का मूल्यांकन करने के लिए कार्यान्वित किया जाता है। क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखन द्रुतान्वेषण फलन) डेटा ऑब्जेक्ट के चेकसम मान को उत्पन्न करके काम करते हैं। यदि डेटा जानबूझकर या अनजाने में संशोधित किया गया है, तो चेकसम मान बदल दिया जाता है। इस प्रकार, डेटा ऑब्जेक्ट की अखंडता का मूल्यांकन पिछले और वर्तमान चेकसम की तुलना और पुष्टि करके किया जा सकता है।

क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखन द्रुतान्वेषण फलन) में किसी भी क्रिप्टोक्लास्टिक हमले के विरूद्व लचीलापन सुनिश्चित करने के लिए पूर्व–छवि प्रतिरोध, द्वितीय पूर्व–छवि प्रतिरोध और टकराव प्रतिरोध गुण प्रदर्शित करना चाहिए।

हैश फंक्शन (द्रुतान्वेषण फलन) बेहद उपयोगी होते हैं और लगभग सभी सूचना सुरक्षा अनुप्रयोगों में दिखाई देते हैं। हैश फंक्शन (द्रुतान्वेषण फलन) एक गणितीय फलन है जो संख्यात्मक इनपुट मान को दूसरे संपीड़ित संख्यात्मक मान में परिवर्तित करता है। हैश फंक्शन (द्रुतान्वेषण फलन) का इनपुट मनमानी लंबाई का है, लेकिन आउटपुट सदैव निश्चित लंबाई का होता है। हैश फंक्शन (द्रुतान्वेषण फलन) द्वारा लौटाए गए मानों को संदेश डाइजेस्ट या केवल हैश मान कहा जाता है।

6.2 हैश फंक्शन (द्रुतान्वेषण फलन) की विशेषतायें :

हैश फंक्शन (द्रुतान्वेषण फलन) की विशेषताएं निम्न हैं –

1. नियत लंबाई का आउटपुट–हैश (निर्गत–द्रुतान्वेषण) मान:

- हैश फंक्शन (द्रुतान्वेषण फलन) किसी भी लंबाई के डेटा को एक निश्चित लंबाई तक ढक करता है। इस प्रक्रिया को अक्सर डेटा हैशिंग (आँकड़ा द्रुतान्वेषण) कहा जाता है।
- सामान्य तौर पर, हैश इनपुट (द्रुतान्वेषण निवेश) डेटा की तुलना में बहुत छोटा है, इसलिए हैश फंक्शन (द्रुतान्वेषण फलन) को कभी–कभी संपीड़न फलन कहा जाता है।
- चूंकि हैश (द्रुतान्वेषण) एक बड़े डेटा का एक छोटा प्रतिनिधित्व है, इसलिए इसे एक पाचन के रूप में भी जाना जाता है।
- n-बिट आउटपुट के साथ हैश फंक्शन (द्रुतान्वेषण फलन) को n–बिट हैश फंक्शन (द्रुतान्वेषण फलन) के रूप में संदर्भित किया जाता है। लोकप्रिय हैश फंक्शन (द्रुतान्वेषण फलन) 160 और 512 बिट्स के बीच मान उत्पन्न करते हैं।

2. संक्रिया की दक्षता:

- आम तौर पर इनपुट x के साथ किसी भी हैश फंक्शन (द्रुतान्वेषण फलन) h के लिए, $h(x)$ की गणना एक तीव्र संक्रिया है।

- सममित एन्क्रिप्शन (कूट प्रक्रिया) की तुलना में संगणन हैश फंक्शन (द्रुतान्वेषण फलन) बहुत तीव्र है।

6.3 हैश फंक्शन (द्रुतान्वेषण फलन) के प्रगुण:

आदर्श क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) में निम्न पाँच मुख्य गुण होते हैंः

- यह नियतात्मक है, जिसका अर्थ है कि एक ही संदेश हमेशा एक ही हैश (द्रुतान्वेषण) में परिणाम देता है।
- किसी भी संदेश के लिए हैश (द्रुतान्वेषण) मान की गणना करना त्वरित है।
- यह व्यावहारिक रूप से संदेश को जनित करने के लिए अव्यवहार्य है जो कि एक दिया गया हैश (द्रुतान्वेषण) मान देता है।
- एक संदेश में किया गया एक छोटा सा परिवर्तन हैश (द्रुतान्वेषण) मान को इतने बड़े पैमाने पर बदलना चाहिए कि नया हैश मान पुराने हैश (द्रुतान्वेषण) मान के साथ असंबंधित दिखाई दे।
- यह एक ही हैश (द्रुतान्वेषण) मान के साथ दो अलग–अलग संदेश खोजने के लिए संभव है।

एक प्रभावी क्रिप्टोग्राफिक (कूटलेखीय) उपकरण होने के लिए, हैश फंक्शन (द्रुतान्वेषण फलन) में निम्नलिखित गुण होने चाहिए है–

संगणनीय रूप से दक्षः

सबसे पहले और सबसे महत्वपूर्ण, हैश फंक्शन (द्रुतान्वेषण फलन) को संगणनीय रूप से कुशल होना चाहिए। अर्थात् कम्प्यूटर को बेहद कम समय में हैश फंक्शन (द्रुतान्वेषण फलन) के गणितीय रूप का प्रदर्शन करने में सक्षम होना चाहिए।

यह गुण शायद कुछ हद तक स्पष्ट है। यदि एक साधारण कम्प्यूटर को क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) को संसाधित करने और आउटपुट (निर्गत) प्राप्त करने के लिए कई मिनटों की आवश्यकता होती है, तो यह बहुत व्यावहारिक नहीं होगा। उपयोगी होने के लिए, हैश फंक्शन (द्रुतान्वेषण फलन) को संगणनीय रूप से कुशल होना चाहिए।

वास्तव में, यह उतनी बड़ी चिंता का विषय नहीं है जितना 40 या 50 साल पहले था। वर्तमान में, एक औसत घरेलू कम्प्यूटर एक सेकंड के छोटे से हिस्से में एक उन्नत हैश फंक्शन (द्रुतान्वेषण फलन) को संसाधित कर सकता है।

नियतात्मकः

क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) नियतात्मक होना चाहिए। अन्य शब्दों में, किसी भी इनपुट (निवेश) के लिए, हैश फंक्शन (द्रुतान्वेषण फलन) को हमेशा समान परिणाम देना चाहिए। यदि हम एक पंक्ति में एक ही इनपुट (निवेश) दस मिलियन बार डालते हैं, तो एक हैश फंक्शन (द्रुतान्वेषण फलन) को दस लाख बार एक ही सटीक आउटपुट का उत्पादन करना चाहिए।

यह भी बल्कि स्पष्ट हो सकता है। यदि एक क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) अलग–अलग आउटपुट का उत्पादन करने के लिए था, तो प्रत्येक बार एक ही इनपुट (निवेश) दर्ज किया गया था, तब हैश फंक्शन (द्रुतान्वेषण फलन) यादृच्छिक होगा और इसलिए अनुपयोगी होगा। एक विशिष्ट इनपुट (निवेश) को सत्यापित करना असंभव होगा, जो हैश फंक्शन (द्रुतान्वेषण फलन) का संपूर्ण बिंदु है – यह सत्यापित करने में सक्षम होने के लिए कि व्यक्तिगत कुंजी तक पहुँच के बिना एक व्यक्तिगत डिजिटल (अंकीय) हस्ताक्षर प्रामाणिक है।

पूर्व–छवि प्रतिरोधः

इस गुण का अर्थ है कि हैश फंक्शन (द्रुतान्वेषण फलन) को व्युत्क्रम करने के लिए संगणनीय रूप से कठिन होना चाहिए। अन्य शब्दों में, यदि हैश फंक्शन (द्रुतान्वेषण फलन) h हैश (द्रुतान्वेषण) मान z का उत्पादन करता है, तो किसी भी इनपुट (निवेश) मान x को प्राप्त करने के लिए एक कठिन प्रक्रिया होनी चाहिए जो कि z पर प्रतिबिम्बित है। यह गुण एक हमलावर के विरूद्व सुरक्षा करती है, जिसके पास केवल एक हैश (द्रुतान्वेषण) मान है और इनपुट (निवेश) खोजने की कोशिश कर रहा है।

द्वितीय पूर्व–छवि प्रतिरोध:

इस गुण का अर्थ है कि दिया गया इनपुट (निवेश) और उसका हैश (द्रुतान्वेषण), एक ही हैश (द्रुतान्वेषण) के साथ एक पृथक इनपुट (निवेश) खोजना मुश्किल होना चाहिए। अन्य शब्दों में, यदि किसी इनपुट (निवेश) x के लिए कोई हैश फंक्शन (द्रुतान्वेषण फलन) h हैश (द्रुतान्वेषण) मान $h(x)$ उत्पन्न करता है, तो किसी अन्य इनपुट (निवेश) मान y को प्राप्त करना कठिन होना चाहिए इस प्रकार कि $h(y) = h(x)$। हैश फंक्शन (द्रुतान्वेषण फलन) का यह गुण उस हमलावर के विरूद्व सुरक्षा करता है जिसके पास इनपुट (निवेश) मान और उसका हैश है, और मूल इनपुट (निवेश) मान के स्थान पर पृथक–पृथक मान को वैध मान के रूप में स्थानापन्न करना चाहता है।

टकराव प्रतिरोध:

इस गुण का अर्थ है कि किसी भी लम्बाई के दो पृथक–पृथक इनपुट्स (निवेश) को प्राप्त करना कठिन होना चाहिए जिसके परिणामस्वरूप एक ही हैश (द्रुतान्वेषण) हो। इस गुण को टकराव मुक्त हैश फंक्शन (द्रुतान्वेषण फलन) के रूप में भी जाना जाता है।

अन्य शब्दों में, हैश फंक्शन (द्रुतान्वेषण फलन) h के लिए, किसी भी दो पृथक–पृथक इनपुट्स (निवेश) x और y को प्राप्त करना कठिन है, जैसे कि इस प्रकार कि $h(y) = h(x)$।

चूंकि, हैश फंक्शन (द्रुतान्वेषण फलन) निश्चित हैश (द्रुतान्वेषण) लंबाई के साथ एक संपीड़ित फंलन है, अतः हैश फंक्शन (द्रुतान्वेषण फलन) के लिए टकराव नहीं होना असंभव है। टकराव मुक्त का यह गुण केवल पुष्टि करता है कि इन टकरावों को खोजना मुश्किल होना चाहिए।

यह गुण एक हमलावर के लिए एक ही हैश (द्रुतान्वेषण) के साथ दो इनपुट (निवेश) मानों को खोजने के लिए बहुत कठिन बनाता है। इसके अतिरिक्त, यदि कोई हैश फंक्शन (द्रुतान्वेषण फलन) टकराव–प्रतिरोधी है, तो यह द्वितीय पूर्व–छवि प्रतिरोधी है।

टकराव प्रतिरोध का अर्थ है द्वितीय पूर्व–छवि प्रतिरोध, लेकिन पूर्व–छवि प्रतिरोध का अर्थ नहीं है। सैद्धांतिक क्रिप्टोग्राफी (कूटलेखन) में कमजोर धारणा को हमेशा पसंद किया जाता है, लेकिन व्यवहार में, एक हैश–फंक्शन (द्रुतान्वेषण फलन) जो केवल द्वितीय पूर्व–छवि प्रतिरोधी है असुरक्षित माना जाता है और इसलिए वास्तविक अनुप्रयोगों के लिए अनुशंसित नहीं है।

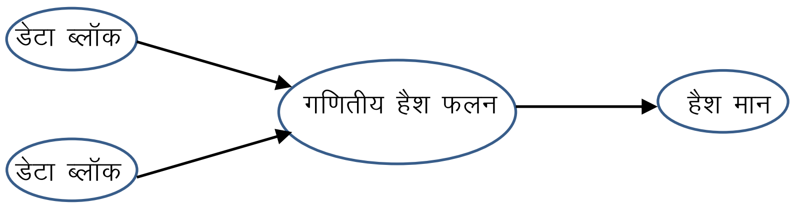
अनौपचारिक रूप से, इन गुणों का अर्थ है कि एक दुर्भावनापूर्ण विरोधी अपने पाचन को परिवर्तित किये बिना इनपुट डेटा (निवेश आँकड़ा) को प्रतिस्थापित या संशोधित नहीं कर सकता है। इस प्रकार, यदि दो स्ट्रिंग्स में एक ही पाचन होता है, तो एक बहुत आश्वस्त हो सकता है कि वे समान हैं। द्वितीय पूर्व–छवि प्रतिरोध एक हमलावर को उसी हैश (द्रुतान्वेषण) के साथ दस्तावेज में चालाकी करने से रोकता है, जैसा कि हमलावर नियंत्रित नहीं कर सकता। टकराव प्रतिरोध एक हमलावर को एक ही हैश (द्रुतान्वेषण) के साथ दो पृथक–पृथक दस्तावेज बनाने से रोकता है।

इन मानदंडों को पूरा करने वाले एक फलन में अभी भी अवांछनीय गुण हो सकते हैं। वर्तमान में लोकप्रिय क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) लंबाई–विस्तार हमलों के लिए असुरक्षित हैं। दिए गए $hash(m)$ और $len(m)$ लेकिन m नहीं, एक उपयुक्त m' का चयन करके एक हमलावर $hash(m \| m')$ की गणना कर सकता है जहाँ $\|$ संयोजन को द्योतित करता है। इस गुण का उपयोग हैश फंक्शन (द्रुतान्वेषण फलन) के आधार पर अनुभवहीन प्रमाणीकरण योजनाओं को तोड़ने के लिए किया जा सकता है। HMAC निर्माण इन समस्याओं के आसपास काम करता है।

व्यवहार में, कई व्यावहारिक उपयोगों के लिए टक्कर प्रतिरोध अपर्याप्त है। टकराव प्रतिरोध के अतिरिक्त, एक विरोधी के लिए दो संदेश काफी हद तक समान पाचन के साथ खोजना असंभव होना चाहिए; या डेटा के बारे में किसी भी उपयोगी जानकारी का अनुमान लगाने के लिए, केवल उसका पाचन दिया गया हो। विशेष रूप से, एक हैश फंक्शन (द्रुतान्वेषण फलन) को एक यादृच्छिक फलन (अक्सर सुरक्षा के प्रमाणों में एक यादृच्छिक ओरेकल कहा जाता है) के समान जितना संभव हो उतना व्यवहार करना चाहिए, जबकि अभी भी निर्धारक और कुशलतापूर्वक संगणनीय होना चाहिए। यह SWIFFT फलन जैसे कार्यों को नियमबद्ध करता है, जो कि टकराव प्रतिरोधी साबित होने के लिए कड़ाई से साबित हो सकता है कि आदर्श जालकों पर कुछ समस्याएं कम्प्यूटेशनल रूप से कठिन हैं, लेकिन एक रैखिक फलन के रूप में, इन अतिरिक्त गुणों को संतुष्ट नहीं करता है।

6.4 हैशिंग एल्गोरिथ्म (द्रुतान्वेषण कलनविधि) की अभिकल्पना:

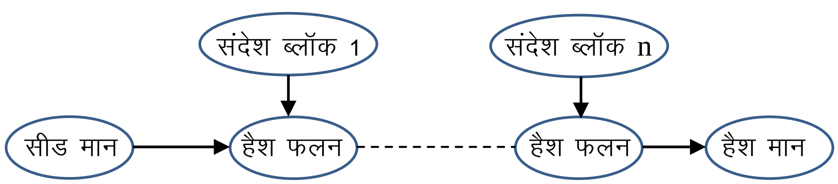
हैशिंग (द्रुतान्वेषण) के केंद्र में एक गणितीय फलन है जो हैश (द्रुतान्वेषण) कोड बनाने के लिए डेटा के दो निश्चित आकार के ब्लॉक पर संचालित होता है। यह हैश फंक्शन (द्रुतान्वेषण फलन) हैशिंग एल्गोरिथ्म (द्रुतान्वेषण कलनविधि) का हिस्सा बनाता है। प्रत्येक डेटा ब्लॉक का आकार एल्गोरिथ्म (कलनविधि) के आधार पर भिन्न होता है। आमतौर पर ब्लॉक का आकार 128 बिट से 512 बिट्स तक होता है। निम्नलिखित चित्रण हैश फंक्शन (द्रुतान्वेषण फलन) को प्रदर्शित करता है –



(चित्र क्र0 6.1)

हैशिंग एल्गोरिथ्म (द्रुतान्वेषण कलनविधि) में ब्लॉक सिफर (खण्ड कूटलेख) के समान उपरोक्त हैश फंक्शन (द्रुतान्वेषण फलन) के चक्र सम्मिलित हैं। प्रत्येक चक्र एक निश्चित आकार का इनपुट (निवेश) लेता है, आमतौर पर सबसे हाल के संदेश ब्लॉक का संयोजन और अंतिम चक्र का आउटपुट (निर्गत)।

इस प्रक्रिया को पूरे संदेश को हैश (द्रुतान्वेषण) करने के लिए आवश्यक रूप में कई चक्र के लिए दोहराया जाता है। हैशिंग एल्गोरिथ्म (द्रुतान्वेषण कलनविधि) के योजनाबद्ध को निम्न चित्रण में दर्शाया गया है–



(चित्र क्र0 6.2)

चूंकि, प्रथम संदेश ब्लॉक का हैश (द्रुतान्वेषण) मान द्वितीय हैश संक्रिया के लिए एक इनपुट (निवेश) बन जाता है, जिसमें से आउटपुट तृतीय संक्रिया के परिणाम को बदल देता है, और इसी तरह। यह प्रभाव, हैशिंग (द्रुतान्वेषण) के हिमस्खलन प्रभाव के रूप में जाना जाता है। यह प्रभाव दो संदेशों के लिए अलग–अलग हैश (द्रुतान्वेषण) मानों में होता है जो डेटा के एक बिट से भिन्न होते हैं।

हैश फंक्शन (द्रुतान्वेषण फलन) और एल्गोरिथ्म (कलनविधि) के मध्य अंतर को सही ढंग से समझें। हैश फंक्शन (द्रुतान्वेषण फलन) निश्चित लंबाई वाले बाइनरी डेटा के दो ब्लॉक्स पर कार्य करके एक हैश (द्रुतान्वेषण) कोड उत्पन्न करता है। हैशिंग एल्गोरिथ्म (द्रुतान्वेषण कलनविधि) हैश फंक्शन (द्रुतान्वेषण फलन) का उपयोग करने के लिए एक प्रक्रिया है, यह निर्दिष्ट करता है कि संदेश कैसे टूट जाएगा और पिछले संदेश ब्लॉक से परिणाम एक साथ कैसे श्रृंखलाबद्व किए जाते हैं।

मर्कले–डैमेज संरचना:

एक हैश फंक्शन (द्रुतान्वेषण फलन) निश्चित लंबाई के आउटपुट में एक स्वेच्छ लंबाई वाले संदेश को संसाधित करने में सक्षम होना चाहिए। यह समान आकार के ब्लॉक्स की एक श्रृंखला में इनपुट (निवेश) को तोड़कर, और एक–तरफा संपीड़न फलन का उपयोग करके अनुक्रम में उन पर कार्य करके प्राप्त किया जा सकता है। संपीड़न फलन या तो विशेष रूप से हैशिंग (द्रुतान्वेषण) के लिए अभिकल्पित किया जा सकता है या ब्लॉक सिफर (खण्ड कूटलेख) से बनाया जा सकता है।

मर्कले–डैमेज संरचना के साथ बनाया गया एक हैश फंक्शन (द्रुतान्वेषण फलन) टकरावों के लिए उतना ही प्रतिरोधी है जितना कि इसका संपीड़न कार्य। पूर्ण हैश फंक्शन (द्रुतान्वेषण फलन) के लिए किसी भी टकराव का पता संपीड़न फलन में टकराव से लगाया जा सकता है।

संसाधित किया गया अंतिम ब्लॉक भी स्पष्ट रूप से लंबा होना चाहिए। यह इस संरचना की सुरक्षा के लिए महत्वपूर्ण है। इस संरचना को मर्कले–डैमेज संरचना कहा जाता है। SHA-1 और MD5 सहित अधिकांश सामान्य क्लासिकल हैश फंक्शन (द्रुतान्वेषण फलन) इस रूप को लेते हैं।

अधिकांश व्यावहारिक हैश फंक्शन (द्रुतान्वेषण फलन) मर्कले–डैमगार्ड संरचना का उपयोग करते हैं, जो संदेश M को नियत लंबाई के ब्लॉक $M_1, M_2,\ldots$ आदि में बांटता है, अंतिम ब्लॉक को पैड करता है और संदेश की लंबाई को अंतिम ब्लॉक में जोड़ता है। परिणामी अंतिम ब्लॉक (सभी पैडिंग के बाद) को M_n द्वारा द्योतित किया जाता है। फिर, हैश फंक्शन (द्रुतान्वेषण फलन) क्रमिक रूप से प्रत्येक ब्लॉक पर टकराव मुक्त फलन H लागू करता हैः

फलन H इनपुट (निवेश) के रूप में पिछले ब्लॉक (या पहले ब्लॉक में एक निश्चित प्रारंभिक मूल्य IV) पर H के अनुप्रयोग के परिणाम को लेता है, और ब्लॉक स्वयं भी, और एक हैश (द्रुतान्वेषण) मान में परिणाम देता है। हैश (द्रुतान्वेषण) मान अगले ब्लॉक पर H के अनुप्रयोग के लिए एक इनपुट है।

हैश फंक्शंस (द्रुतान्वेषण फलन) अंतिम ब्लॉक पर H का परिणाम संदेश h(M) का हैशेड (द्रुतान्वेषण) मान हैः

$$h_0 = IV = \text{नियत प्रारंभिक मान}$$
$$h_1 = H(h_0,M_1)$$
$$\ldots$$
$$h_i = H(hi-1,Mi)$$
$$h_n = H(h_{n-1},M_n)$$
$$h(M) = h_n$$

यदि H टकराव मुक्त है, तो h भी टकराव मुक्त है।

वाइड पाइप विरूद्व संकीर्ण पाइपः

यह मर्कले–डैमेगार्ड संरचना का एक सीधा अनुप्रयोग है, जहाँ हैश (द्रुतान्वेषण) आउटपुट (निर्गत) का आकार आंतरिक स्थिति के आकार (प्रत्येक संपीड़न चरण के मध्य) के समान होता है, जिसके परिणामस्वरूप एक संकीर्ण–पाइप हैश (द्रुतान्वेषण) अभिकल्पना होता है। यह अभिकल्पना कई अंतर्निहित त्रुटियों का कारण बनता है, जिसमें लंबाई–विस्तार, बहु–टकराव, लंबे संदेश हमले, जनित और चिपकाए गए हमले शामिल हैं, और इसे समानांतर भी नहीं किया जा सकता है। परिणामतः, आधुनिक हैश फंक्शंस (द्रुतान्वेषण फलन) चौड़े पाइप संरचनां पर बनाए जाते हैं, जिनमें आंतरिक आकार बड़ा होता है, जो कि मर्कले–डैमगार्ड संरचना से लेकर नई संरचना जैसे स्पोंज संरचना और HAIFA संरचना तक होते हैं।

6.5 प्रसिद्व हैश फंक्शन (द्रुतान्वेषण फलन):

कुछ प्रसिद्व हैश फंक्शन (द्रुतान्वेषण फलन) निम्न हैंः

6.5.1 मैसेज डाइजेस्ट (संदेश संग्रह) (MD):

MD5 अत्यंत लोकप्रिय था और व्यापक रूप से कई वर्षों तक हैश फंक्शन (द्रुतान्वेषण फलन) का उपयोग किया जाता था। एमडी परिवार में हैश फंक्शन (द्रुतान्वेषण फलन) MD2, MD4, MD5 और MD6 सम्मिलित हैं। इसे इंटरनेट स्टैंडर्ड RFC 1321के रूप में अपनाया गया था। यह 128–बिट हैश फंक्शन (द्रुतान्वेषण फलन) है।

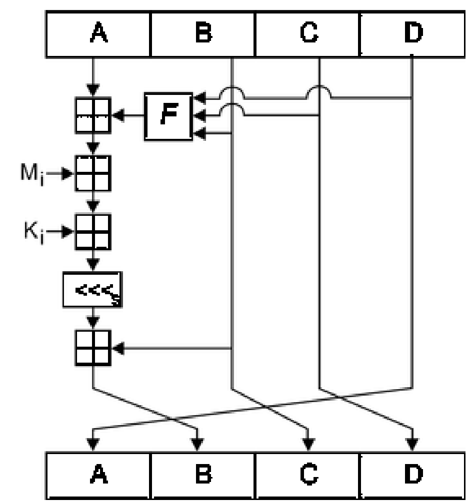
सॉफ्टवेयर की दुनिया में MD5 डाइजेस्ट का व्यापक रूप से उपयोग किया गया है ताकि हस्तांतरित फाइल की अखंडता के बारे में आश्वासन दिया जा सके। उदाहरण के लिए, फाइल सर्वर अक्सर फाइल्स के लिए एक पूर्व–संग्रहीत MD5 चेकसम प्रदान करते हैं, ताकि उपयोगकर्ता डाउनलोड की गई फाइल के चेकसम की तुलना कर सके।

2004 में, MD5 में टकराव पाया गया। एक विश्लेषणात्मक हमले को कम्प्यूटर क्लस्टर का उपयोग करके केवल एक घंटे में सफल होने की सूचना दी गई थी। इस टक्कर के हमले के परिणामस्वरूप MD5 समझौता हो गया और इसलिए इसे अब उपयोग के लिए अनुशंसित नहीं किया गया है। MD5 व्यापक रूप से उपयोग किया जाने वाला क्रिप्टोग्राफिक हैश फंक्शन है (कूटलेखन द्रुतान्वेषण फलन) जो 128–बिट (16–बाइट) हैश (द्रुतान्वेषण) मान का उत्पादन करता है। RFC 1321 में निर्दिष्ट, MD5 को विभिन्न प्रकार के सुरक्षा अनुप्रयोगों में नियोजित किया गया है, और इसका उपयोग आमतौर पर डेटा अखंडता की जांच के लिए भी किया जाता है। हालांकि, यह दिखाया गया है कि MD5 टक्कर प्रतिरोधी नहीं है। क्रिप्टोग्राफर्स (कूटलेखक) ने अन्य एल्गोरिथ्म (कलनविधि) के उपयोग की सिफारिश करना शुरू किया, जैसे कि SHA-1 (जो तब से पाया गया है, जो असुरक्षित भी है)। अधिकांश अमेरिकी सरकारी अनुप्रयोगों को अब हैश (द्रुतान्वेषण) कार्यों के SHA-2 परिवार की आवश्यकता होती है।

MD5 एक चर–लंबाई वाले संदेश को 128–बिट्स की नियत–लंबाई वाले आउटपुट में संसाधित करता है। सबसे पहले, इनपुट संदेश को 512–बिट ब्लॉक्स के टुकड़े में तोड़ दिया जाता है, संदेश पैडेड है अतः इसकी लंबाई 512 से विभाज्य है।

बाद में, एक 128–बिट अवस्था, जिसे A, B, C और D नाम के चार 32–बिट शब्दों में विभाजित किया गया है, को कुछ नियत स्थिरांक के लिए आरंभीकृत किया जाता है।

मुख्य एल्गोरिथ्म (कलनविधि) फिर प्रत्येक 512–बिट संदेश ब्लॉक को संचालित करता है, प्रत्येक ब्लॉक अवस्था को संशोधित करता है। एक संदेश ब्लॉक के प्रसंस्करण में चार समान चरण होते हैं, जिन्हें चक्र कहा जाता है। प्रत्येक चक्र 16 समान संचालन से बना होता है जो एक अरैखिक फलन F, मॉड्यूलर योग और बाएं घूर्णन पर आधारित होता है। निम्न चित्र एक चक्र के अंदर होने वाली संक्रिया को दिखाता है।



(चित्र क्र0 6.3; स्त्रोतः इंटरनेट से साभार)

M_i संदेश इनपुट (निवेश) के 32–बिट ब्लॉक को दर्शाता है, और K_i प्रत्येक संक्रिया के लिए पृथक 32–बिट स्थिरांक को दर्शाता है। $\lll_s$, s स्थान बायीं ओर बिट घूर्णन को द्योतित करता है। s प्रत्येक संक्रिया के लिए भिन्न होता है। $\boxplus$ योग मॉडुलो 2^{32} को दर्शाता है। चार संभावित फलन F, G, H, I होते हैं, प्रत्येक चक्र में पृथक फलन का उपयोग किया जाता है।

$$F(X,Y,Z) = (X \wedge Y) \vee (\sim X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \backsim Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \backsim Z)$$

$\oplus, \wedge, \vee, \backsim$ क्रमशः XOR, AND, OR और NOT संक्रिया को दर्शाता है।

6.5.2 सुरक्षित हैश फंक्शन (द्रुतान्वेषण फलन) (SHA):

SHA परिवार में चार SHA एल्गोरिथ्म (कलनविधि) सम्मिलित हैं, SHA-0, SHA-1, SHA-2 और SHA-3। हालांकि एक ही परिवार से हैं लेकिन संरचनात्मक रूप से पृथक हैं। मूल संस्करण SHA-0 है, एक 160–बिट हैश फंक्शन (द्रुतान्वेषण फलन) जिसे 1993 में राष्ट्रीय मानक और प्रौद्योगिकी संस्थान द्वारा प्रकाशित किया गया था। इसकी कुछ कमियाँ थीं और यह बहुत लोकप्रिय नहीं हुआ। बाद में 1995 में, SHA-1 को SHA-0 की कथित कमियों को ठीक करने के लिए डिजाइन किया गया था।

SHA-1 उपलब्ध SHA हैश फंक्शन (द्रुतान्वेषण फलन) का सबसे व्यापक रूप से उपयोग किये जाने वाला संस्करण है। यह सिक्योर सॉकेट लेयर (Secure Socket Layer - SSL) सुरक्षा सहित कई व्यापक रूप से उपयोग किए जाने वाले अनुप्रयोगों और प्रोटोकॉल में कार्यरत है।

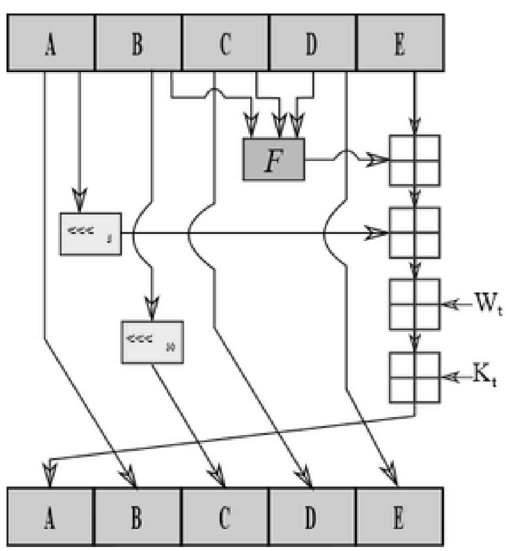
2005 में, SHA-1 के दीर्घावधि रोजगार को संदिग्ध बनाते हुए व्यावहारिक समय सीमा के अंदर SHA-1 के लिए टकराव को उजागर करने के लिए एक विधि पाई गई।

SHA-2 परिवार के चार और SHA संस्करण हैं, SHA-224, SHA-256, SHA-384 और SHA-512 जो उनके हैश (द्रुतान्वेषण) मान में बिट्स की संख्या पर आधारित हैं। SHA-2 हैश फंक्शन (द्रुतान्वेषण फलन) पर अभी तक कोई सफल हमला नहीं हुआ है।

हालांकि SHA-2 एक मजबूत हैश फंक्शन (द्रुतान्वेषण फलन) है तथा सार्थक रूप से पृथक है। इसकी मूल अभिकल्पना अभी भी SHA-1 की अभिकल्पना का अनुसरण करता है। इसलिए, NIST ने नए प्रतिस्पर्धी हैश फंक्शन (द्रुतान्वेषण फलन) अभिकल्पनाओं को बुलाया।

अक्टूबर 2012 में, NIST ने नए SHA-3 मानक के रूप में केकेक एल्गोरिथ्म (कलनविधि) को चुना। यह कई लाभ प्रदान करता है, जैसे कुशल प्रदर्शन और हमलों के लिए अच्छा प्रतिरोध।

SHA एलगोरिथ्म (कलनविधि): तीन SHA एल्गोरिथ्म (कलनविधि) पृथक विधियों से संरचित होते हैं और इन्हें SHA-0, SHA-1 और SHA-2 के रूप में प्रतिष्ठित किया जाता है। SHA-1, SHA-0 से बहुत मिलता–जुलता है, लेकिन मूल SHA हैश (द्रुतान्वेषण) विनिर्देश में एक त्रुटि को ठीक करता है जिसके कारण महत्वपूर्ण कमियाँ हुईं। SHA-0 एल्गोरिथ्म (कलनविधि) को कई अनुप्रयोगों द्वारा नहीं अपनाया गया था। दूसरी ओर SHA-2, SHA-1 हैश फंक्शन (द्रुतान्वेषण फलन) से काफी भिन्न होता है।



(चित्र क्र0 6.4; स्त्रोतः इंटरनेट से साभार)

SHA-1 चर–लंबाई संदेश को 160–बिट्स की नियत–लंबाई वाले आउटपुट में संसाधित करता है, यह प्रक्रिया MD5 के समान है।

सबसे पहले, इनपुट (निवेश) संदेश को 512—बिट ब्लॉक्स के टुकड़े में तोड़ दिया जाता है, संदेश इस प्रकार पैडेड होता है ताकि इसकी लंबाई 512 तक विभाज्य हो।

द्वितीय यह कि, एक 160—बिट अवस्था, जिसे A, B, C, D और E के रूप में पांच 32—बिट शब्दों में विभाजित किया गया है, जो कुछ नियत स्थिरांक के लिए आरंभिक हैं।

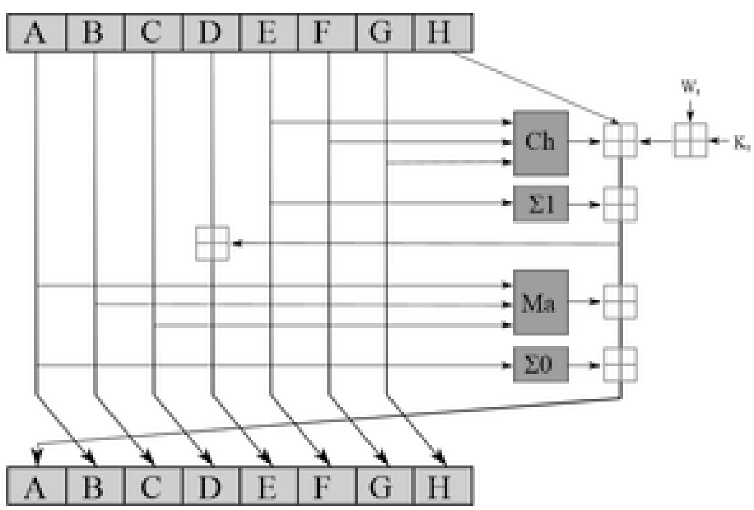
मुख्य एल्गोरिथ्म (कलनविधि) फिर प्रत्येक 512—बिट संदेश ब्लॉक को संचालित करता है, प्रत्येक ब्लॉक अवस्था को संशोधित करता है। एक संदेश ब्लॉक के प्रसंस्करण में पांच समान चरण होते हैं, जिन्हें चक्र कहा जाता है। प्रत्येक चक्र 16 समान संचालन से बना होता है जो एक अ—रैखिक फंक्शन F, मॉड्यूलर योग और बाएं घूर्णन पर आधारित होता है। उपरोक्त चित्र एक चक्र के अंदर होने वाली संक्रिया को दिखाता है।

F एक अ—रैखिक फलन है जो परिवर्तित होता रहता है। $\lll_n$, n स्थान बायीं ओर बिट घूर्णन को द्योतित करता है। n प्रत्येक संक्रिया के लिए भिन्न होता है। W_t चक्र t का विस्तारित संदेश शब्द है। K_t चक्र t का चक्र स्थिरांक है। ⊞ योग मॉडुलो 2^{32} को दर्शाता है।

SHA-2 क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखन द्रुतान्वेषण फलन) (SHA-224, SHA-256, SHA-384, SHA-512) को राष्ट्रीय सुरक्षा एजेंसी द्वारा डिजाइन किया गया है और 2001 में NIST द्वारा एक अमेरिकी संघीय सूचना प्रोसेसिंग मानक के रूप में प्रकाशित किया गया है। SHA-2 में अपने पूर्ववर्ती SHA-1 के महत्वपूर्ण परिवर्तन शामिल हैं। SHA-2 में 224, 256, 384 या 512 बिट्स वाले डाइजेस्ट के साथ चार हैश फंक्शंस (द्रुतान्वेषण फलन) का एक समूह होता है।

SHA-256 और SHA-212 क्रमशः 32 और 64 बिट शब्दों के साथ संगणित हैश फंक्शन (द्रुतान्वेषण फलन) हैं। वे पृथक—पृथक शिफ्ट राशियों और योगात्मक स्थिरांक का उपयोग करते हैं, लेकिन उनकी संरचनाएं लगभग समान हैं, केवल चक्र की संख्या में भिन्न हैं। SHA-224 और SHA-384 केवल शुरुआती दो के खण्डित संस्करण हैं, जिनकी विभिन्न प्रारंभिक मूल्यों के साथ गणना की जाती है।

इस बिंदु पर, हमें पहले से ही समझना चाहिए कि MD5, SHA1 कैसे काम करता है, इसलिए यहाँ SHA-2 के प्रसंस्करण आरेख को नीचे दिया गया है।



(चित्र क्र0 6.5; स्त्रोतः इंटरनेट से साभार)

SHA-2 में निम्न संक्रियायें होती हैं:

$$C_h(E,F,G) = (E \wedge F) \oplus (\sim E \wedge G)$$
$$M_a(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\textstyle\sum_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\textstyle\sum_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

बिटवाइज घूर्णन SHA–512 के लिए विभिन्न स्थिरांक का उपयोग करता है। दी गई संख्या SHA–256 के लिए हैं। ⊞ योग मॉडुलो 2^{32} को दर्शाता है।

SHA–2 मूल रूप से दो हैश एल्गोरिथ्म (द्रुतान्वेषण कलनविधि) रखते हैं: SHA–256 और SHA–512। SHA–224 पृथक–पृथक शुरुआती मानों और खण्डित वाले आउटपुट के साथ SHA–256 का एक प्रकार है। SHA–384 और कम ज्ञात SHA–512/224 और SHA-512/256 SHA–512 के सभी प्रकार हैं। SHA–512 SHA–256 की तुलना में अधिक सुरक्षित है और यह AMD64 जैसी 64 बिट मशीनों पर SHA–256 की तुलना में अधिक तीव्र है।

बिट्स में आउटपुट (निर्गत) का आकार SHA नाम के विस्तार द्वारा दिया जाता है। इसलिए SHA–224 का आउटपुट आकार 224 बिट्स (28 बाइट्स) होता है। SHA–256 32 बाइट्स का उत्पादन करता है। SHA–384 48 बाइट्स का उत्पादन करता है और अंत में SHA–512 64 बाइट का उत्पादन करता है।

SHA–3 NIST द्वारा 5 अगस्त 2015 को जारी किया गया था। SHA–3 व्यापक क्रिप्टोग्राफिक (कूटलेखीय) आदिम परिवार केकेक का उपसमूह है। केकेक एल्गोरिथ्म (कलनविधि) गुइडो बर्टोनी, जोन डैमेन, माइकल पीटर्स और गिल्स वान अस्चे का काम है। केकेक एक स्पंज संरचना पर आधारित है, जिसका उपयोग अन्य क्रिप्टोग्राफिक (कूटलेखीय) प्राथमिक जैसे स्ट्रीम सिफर (प्रवाह कूटलेख) बनाने के लिए भी किया जा सकता है। SHA–3, SHA–2 के समान आउटपुट आकार प्रदान करता है, जैसे 224, 256, 384 और 512 बिट्स।

विन्यास आउटपुट आकार को SHAKE-128 और SHAKE-256 कार्यों का उपयोग करके भी प्राप्त किया जा सकता है। यहाँ 128 और 256 नाम एक्सटेंशन बिट्स में आउटपुट आकार के स्थान पर फलन की सुरक्षा ताकत का अर्थ है।

6.5.3 RIPEMD

RIPEND, RACE इंटीग्रिटी प्रिमिटिव इवैल्यूएशन मैसेज डाइजेस्ट का संक्षिप्त नाम है। हैश फंक्शंस (द्रुतान्वेषण फलन) के इस समूह को खुले अनुसंधान समुदाय द्वारा डिजाइन किया गया था और आमतौर पर इसे यूरोपीय हैश फंक्शंस (द्रुतान्वेषण फलन) के परिवार के रूप में जाना जाता था।

समूह में RIPEND, RIPEMD-128 और RIPEMD-160 सम्मिलित हैं। इस एल्गोरिथ्म (कलनविधि) के 256, और 320–बिट संस्करण भी उपलब्ध हैं।

मूल RIPEND (128 बिट) MD4 में उपयोग किए गए अभिकल्पना सिद्धांतों पर आधारित है और इसे संदिग्ध सुरक्षा प्रदान करने के लिए पाया जाता है। RIPEND 128–बिट संस्करण मूल RIPEND पर कमियों को दूर करने के लिए एक त्वरित स्थिर प्रतिस्थापन के रूप में आया था।

RIPEND–160 एक उन्नत संस्करण है और परिवार में सबसे अधिक उपयोग किया जाने वाला संस्करण है। 256 और 320–बिट संस्करण आकस्मिक टकराव की संभावना को कम करते हैं, लेकिन RIPEND–128 और RIPEND–160 की तुलना में उच्च स्तर की सुरक्षा नहीं है।

RIPEND क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) का एक परिवार है, जो हैव, बेल्जियम में हैंस डोबबर्टिन, एंटून बॉसएलेर्स और बार्ट प्रिनेल द्वारा कैथोलिक यूनिवर्स लियवेन में COSS अनुसंधान समूह में विकसित किया गया है, और प्रथम संस्करण 1996 में प्रकाशित हुआ। RIPEND, MD4 में उपयोग किए गए डिजाइन सिद्धांतों के आधार पर, और अधिक लोकप्रिय SHA–1 के प्रदर्शन के समान है। RIPEND–160 को हालांकि नहीं तोड़ा गया है। जैसा कि नाम से ही स्पष्ट है कि RIPEND–160 में 160 बिट्स (20 बाइट्स) का हैश डाइजेस्ट (द्रुतान्वेषण पाचन) होता है।

RIPEMD (RIPE Message Digest) 1992 (मूल RIPEMD) और 1996 (अन्य संस्करण) में विकसित क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) का एक परिवार है। परिवार में पाँच फंक्शन हैं: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, और RIPEMD-320, जिनमें से RIPEMD–160 सबसे सार्व है।

मूल RIPEMD, साथ ही RIPEMD–128, सुरक्षित नहीं माना जाता है क्योंकि 128–बिट परिणाम बहुत छोटा है और अभिकल्पना कमियों के कारण भी (मूल RIPEMD के लिए) है। RIPEMD के 256 और 320–बिट संस्करण क्रमशः RIPEMD–128 और RIPEMD–160 के समान सुरक्षा प्रदान करते हैं। वे उन अनुप्रयोगों के लिए डिजाइन किए गए हैं जहाँ सुरक्षा स्तर पर्याप्त है, लेकिन अब हैश (द्रुतान्वेषण) परिणाम आवश्यक है।

6.5.4 व्हर्लपूल:

यह 512–बिट हैश फंक्शन (द्रुतान्वेषण फलन) है। इसे AES के संशोधित संस्करण से व्युत्पन्न किया गया है। इसके डिजाइनर AES के सह–निर्माता विन्सेन्ट रिजमेन थे। व्हर्लपूल के तीन संस्करण जारी किए गए हैं, अर्थात् WHIRLPOOL-0, WHIRLPOOL-T और WHIRLPOOL।

कम्प्यूटर विज्ञान और क्रिप्टोग्राफी (कूटलेखन) में, व्हर्लपूल एक क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) है। इसे विन्सेन्ट रिजमेन और पाउलो एस. एल. एम. बैरेटो द्वारा डिजाइन किया गया था, जिन्होंने पहली बार इसे 2000 में वर्णित किया था। व्हर्लपूल AES के अत्यंत संशोधित संस्करण पर आधारित है। व्हर्लपूल 512 बिट्स (64 बाइट्स) का हैश डाइजेस्ट (द्रुतान्वेषण पाचन) उत्पन्न करता है।

NESSIE परियोजना द्वारा हैश (द्रुतान्वेषण)की सिफारिश की गई है। यह अंतर्राष्ट्रीय संगठन मानकीकरण (ISO) और अंतर्राष्ट्रीय इलेक्ट्रोटेक्निकल कमीशन (IEC) द्वारा संयुक्त ISO/IEC 10118–3 अंतर्राष्ट्रीय मानक के हिस्से के रूप में भी अपनाया गया है।

व्हर्लपूल एक हैश फंक्शन (द्रुतान्वेषण फलन) है जिसे स्क्वायर ब्लॉक सिफर (वर्ग खण्ड कूटलेख) के बाद डिजाइन किया गया, और ब्लॉक सिफर (खण्ड कूटलेख) फलन के परिवार में माना जाता है। व्हर्लपूल एक मियागुची–प्रिनेल संरचना है जो अत्यंत संशोधित AES पर आधारित है। व्हर्लपूल 2^{256} बिट्स से कम किसी भी लंबाई का संदेश लेता है और 512–बिट मैसेज डाइजेस्ट (द्रुतान्वेषण पाचन) को वापस करता है।

संस्करणः

मूल व्हर्लपूल को WHIRLPOOL-0 कहा जाएगा, व्हर्लपूल के पहले संशोधन को WHIRLPOOL-T कहा जाएगा और नवीनतम संस्करण को निम्नलिखित परीक्षण सदिश में WHIRLPOOL कहा जाएगा।

2001 में पहले संशोधन में, S–बॉक्स को यादृच्छिक ढंग से उत्पन्न क्रिप्टोग्राफिक (कूटलेखीय) गुणों वाले एक बॉक्स से बदल दिया गया था, जिसमें क्रिप्टोग्राफिक (कूटलेखीय) गुण बेहतर हैं और हार्डवेयर में लागू करना आसान है।

दूसरे संशोधन (2003) में, प्रसार आव्यूह में एक दोष पाया गया था जो कि इसकी क्षमता के नीचे एल्गोरिथ्म (कलनविधि) की अनुमानित सुरक्षा को कम करता था। (1, 1, 3, 1, 5, 8, 9, 5) से (1, 1, 1, 4, 1, 8, 5, 2, 9) तक 8 × 8 घूर्णन आव्यूह स्थिरांक को परिवर्तित करते हुए इस समस्या को हल किया जाता है।

आंतरिक संरचनाः

ब्लॉक सिफर (खण्ड कूटलेख) W बाइट्स के 8 × 8 आव्यूह S को रखता है, कुल 512 बिट्स के लिए। एन्क्रिप्शन प्रक्रिया 10 चक्र के ऊपर चार चक्र फंक्शन के साथ अवस्था को अद्यतन करता है। चार चक्र फलन SubBytes (SB), ShiftColumns (SC), MixRows (MR) और AddRoundKey (AK) हैं। प्रत्येक चक्र के दौरान नई अवस्था की गणना S = AKoMRoSCoSB(S)½ के रूप में की जाती है।

सब–बाइट्स (SB): सब–बाइट्स (SB) संक्रिया स्वतंत्र रूप से अवस्था के प्रत्येक बाइट के लिए एक अ–रैखिक क्रमपरिवर्तन (S–बॉक्स) लागू करता है। 8–बिट S–बॉक्स को 3 छोटे 4–बिट S–बॉक्स से बनाया जाता है।

विस्थापित–स्तंभ (SC): विस्थापित–स्तंभ (SC) संक्रिया अवस्था के प्रत्येक स्तंभ में प्रत्येक बाइट को चक्रीय रूप से बदलता है। कॉलम j की अपनी बाइट्स को j स्थिति नीचे की ओर स्थानांतरित करता है।

मिश्रित–पंक्ति (MR): मिश्रित–पंक्ति (MR) संक्रिया, $GF(2^8)$ के ऊपर 8 × 8 आव्यूह द्वारा प्रत्येक पंक्ति का एक सही गुणन है। आव्यूह को ऐसा चुना जाता है कि शाखा संख्या (एक महत्वपूर्ण गुण जब अंतर क्रिप्टोनालिसिस (कूटविश्लेषण) के प्रतिरोध को देखती है) 9 हो, जो कि अधिकतम है।

योग चक्र कुंजी (AK):

योग चक्र कुंजी (AK) संक्रिया वर्तमान अवस्था के लिए कुंजी चक्र द्वारा गणना की गई कुंजी को जोड़ने के लिए बिटवाइज XOR का उपयोग करता है। कुंजी चक्र, एन्क्रिप्शन (कूट प्रक्रिया) के समान है, योग चक्र कुंजी (AK) फलन को छोड़कर जिसे योग चक्र स्थिरांक फलन द्वारा प्रतिस्थापित किया जाता है जो प्रत्येक चक्र में एक पूर्वनिर्धारित स्थिरांक जोड़ता है।

व्हर्लपूल को शामिल करने वाले लोग व्हर्लपूल के सबसे हाल के संशोधन का उपयोग करते हैं, जबकि व्हर्लपूल के पहले संस्करणों में कोई ज्ञात सुरक्षा कमियाँ नहीं हैं। सबसे हाल के संशोधन में बेहतर हार्डवेयर कार्यान्वयन दक्षता विशेषताएं हैं, और अधिक सुरक्षित होने की संभावना है। जैसा कि पहले उल्लेख किया गया है, यह ISO/IEC 10118–3 अंतर्राष्ट्रीय मानक में अपनाया गया संस्करण भी है।

512–बिट (64–बाइट) व्हर्लपूल हैश (जिसे मैसेज डाइजेस्ट भी कहा जाता है) को आमतौर पर 128–अंकीय हेक्साडेसिमल संख्या के रूप में दर्शाया जाता है।

6.6 हैश फंक्शन (द्रुतान्वेषण फलन) के अनुप्रयोग:

हैशिंग (द्रुतान्वेषण) औसत पर स्थिर समय खोज, सम्मिलित और हटाने के संचालन प्रदान करता है। यही कारण है कि हैशिंग (द्रुतान्वेषण) सबसे अधिक उपयोग की जाने वाली डेटा संरचना में से एक है, इसके अनुप्रयोगों में उदाहरण की समस्याएं हैं, पृथक अवयव, वस्तुओं की आवृत्तियों की गणना, प्रतिलिपि की खोज, आदि सम्मिलित हैं।

आधुनिक समय की क्रिप्टोग्राफी (कूटलेखन) में हैश फंक्शन (द्रुतान्वेषण फलन) सहित हैशिंग (द्रुतान्वेषण) के कई अन्य अनुप्रयोग हैं। इन अनुप्रयोगों में से कुछ नीचे सूचीबद्ध हैं:

- मैसेज डाइजेस्ट
- पासवर्ड सत्यापन
- डेटा संरचनाएं (प्रोग्रामिंग भाषाएँ)
- संकलक संक्रिया
- राबिन–कार्प एल्गोरिथ्म (कलनविधि)
- फाइल नाम और पथ को एक साथ जोड़ना

मैसेज डाइजेस्ट:

यह क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखन द्रुतान्वेषण फलन) का एक अनुप्रयोग है। क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखन द्रुतान्वेषण फलन) वे फलन हैं जो एक आउटपुट का उत्पादन करते हैं जिसमें से इनपुट तक पहुंचना असंभव के करीब है। हैश फंक्शंस (द्रुतान्वेषण फलन) के इस गुण को अपरिवर्तनीयता कहा जाता है।

उदाहरण के लिए माना हमें अपनी फाइल्स को उपलब्ध क्लाउड सेवाओं में से किसी पर संग्रहीत करना है। हमें यह सुनिश्चित करना होगा कि हमारे द्वारा संग्रहित फाइल्स को किसी तीसरे पक्ष द्वारा छेड़छाड़ नहीं की जाए। हम क्रिप्टोग्राफिक हैश एल्गोरिथ्म (कूटलेखीय द्रुतान्वेषण कलनविधि) का उपयोग करके उस फाइल के हैश (द्रुतान्वेषण) की गणना करके करते हैं। सामान्य क्रिप्टोग्राफिक हैश एल्गोरिथ्म (कूटलेखीय द्रुतान्वेषण कलनविधि) में से एक SHA 256 है। इस प्रकार गणना किए गए हैश (द्रुतान्वेषण) का अधिकतम आकार 32 बाइट्स है। तो बड़ी संख्या में फाइल्स के हैश (द्रुतान्वेषण) की संगणना कोई समस्या नहीं होगी। हम अपने स्थानीय मशीन पर इन हैश को बचाते हैं।

अब, जब हम फाइल्स को डाउनलोड करते हैं, तो हम फिर से हैश (द्रुतान्वेषण) की गणना करते हैं। फिर हम इसे पिछले हैश (द्रुतान्वेषण) गणना के साथ मिलाते हैं। इसलिए, हम जानते हैं कि हमारी फाइल्स से छेड़छाड़ की गई थी या नहीं। यदि कोई भी फाइल के साथ छेड़छाड़ करता है, तो फाइल का हैश (द्रुतान्वेषण) मान निश्चित रूप से बदल जाएगा। हैश (द्रुतान्वेषण) को बदले बिना फाइल से छेड़छाड़ करना लगभग असंभव है।

पासवर्ड सत्यापनः

पासवर्ड सत्यापन में क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) का आमतौर पर उपयोग किया जाता है। एक उदाहरण का उपयोग करके इसे समझें।

जब आप किसी भी ऑनलाइन वेबसाइट का उपयोग करते हैं जिसके लिए उपयोगकर्ता लॉगिन की आवश्यकता होती है, तो हम यह प्रमाणित करने के लिए अपना ई–मेल और पासवर्ड दर्ज करते हैं कि हम जिस खाते का उपयोग करने का प्रयास कर रहे हैं वह हमारा है। जब पासवर्ड दर्ज किया जाता है, तो पासवर्ड का एक हैश (द्रुतान्वेषण) गणना किया जाता है जो तब पासवर्ड के सत्यापन के लिए सर्वर को भेजा जाता है। सर्वर पर संग्रहीत पासवर्ड वास्तव में मूल पासवर्ड के हैश (द्रुतान्वेषण) मानों की गणना करते हैं। यह सुनिश्चित करने के लिए किया जाता है कि जब पासवर्ड क्लाइंट से सर्वर पर भेजा जाता है, तो कोई आक्रमण करने वाला नहीं है।

पासवर्ड सत्यापन आमतौर पर क्रिप्टोग्राफिक हैश (कूटलेखन द्रुतान्वेषण) पर निर्भर करता है। प्लेन–टेक्स्ट (साधारण–पाठ) के रूप में सभी उपयोगकर्ता पासवर्ड्स को संग्रहीत करने से पासवर्ड फाइल से छेड़छाड़ होने पर बड़े पैमाने पर सुरक्षा भंग हो सकती है। इस खतरे को कम करने की एक विधि केवल प्रत्येक पासवर्ड के हैश डाइजेस्ट (द्रुतान्वेषण पाचन) को संग्रहीत करना है। किसी उपयोगकर्ता को प्रमाणित करने के लिए, उपयोगकर्ता द्वारा प्रस्तुत पासवर्ड को हैश (द्रुतान्वेषण) किया जाता है और संग्रहीत हैश (द्रुतान्वेषण) से तुलना की जाती है। पासवर्ड हैशिंग (द्रुतान्वेषण) करते समय एक पासवर्ड रीसेट विधि की आवश्यकता होती है। मूल पासवर्ड संग्रहीत हैश (द्रुतान्वेषण) मान से पुनर्गणना नहीं किया जा सकता है।

मानक क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) को जल्दी से गणना करने के लिए डिजाइन किया गया है, और, परिणामस्वरूप, उच्च दर पर अनुमानित पासवर्ड का प्रयास करना संभव है। सामान्य ग्राफिक्स प्रोसेसिंग इकाइयाँ प्रत्येक सेकंड में अरबों संभव पासवर्ड की कोशिश कर सकती हैं। पासवर्ड हैश फंक्शंस (द्रुतान्वेषण फलन) जो मुख्य स्ट्रेचिंग करते हैं – जैसे कि PBKDF2, scrypt या Argon2 आमतौर पर समय–समय पर (और कुछ मामलों में कंप्यूटर मेमोरी में) संग्रहित पासवर्ड हैश डाइजेस्ट (द्रुतान्वेषण पाचन) के लिए ब्रूट फोर्स अटैक करने के लिए आवश्यक क्रिप्टोग्राफिक हैश (कूटलेखन द्रुतान्वेषण) का बार–बार उपयोग करते हैं। एक पासवर्ड हैश (द्रुतान्वेषण) को एक बड़े यादृच्छिक, गैर–गुप्त मान के उपयोग की आवश्यकता होती है जिसे पासवर्ड हैश (द्रुतान्वेषण) के साथ संग्रहीत किया जा सकता है। पासवर्ड हैश (द्रुतान्वेषण) के आउटपुट को यादृच्छिक करता है, जिससे पासवर्ड के तालिकाओं को स्टोर करने के लिए एक विरोधी के लिए असंभव हो जाता है और हैश (द्रुतान्वेषण) के मान को पूर्व गणन किया जाता है, जिससे पासवर्ड हैश (द्रुतान्वेषण) की तुलना की जा सकती है।

पासवर्ड हैश फंक्शन (द्रुतान्वेषण फलन) के आउटपुट का उपयोग क्रिप्टोग्राफिक (कूटलेखीय) कुंजी के रूप में भी किया जा सकता है। पासवर्ड हैश (द्रुतान्वेषण) को इसलिए पासवर्ड आधारित कुंजी व्युत्पत्ति फंक्शन (PBKDFs) के रूप में भी जाना जाता है।

डेटा संरचनाएं (प्रोग्रामिंग भाषाएँ):

विभिन्न प्रोग्रामिंग भाषाओं में हैश (द्रुतान्वेषण) तालिका आधारित डेटा संरचनाएं हैं। मूल विचार एक कुंजी–मान जोड़ी बनाना है जहाँ कुंजी को एक अद्वितीय मान माना जाता है, जबकि विभिन्न कुंजी के लिए मान समान हो सकते हैं। यह क्रियान्वयन C ++ में अ–क्रमित समूह और अ–क्रमित प्रतिचित्रण, जावा में हैश–समूह और हैश–प्रतिचित्रण, आदि में देखा जाता है।

संकलक संक्रियाः

एक प्रोग्रामिंग भाषा के कीवर्ड अन्य पहचानकर्ताओं की तुलना में पृथक विधि से संसाधित होते हैं। प्रोग्रामिंग भाषा के कीवर्ड (if, else, for, return आदि) और अन्य पहचानकर्ताओं के मध्य अंतर करने और प्रोग्राम को सफलतापूर्वक संकलित करने के लिए, संकलक इन सभी कीवर्ड्स को एक समूह में रखता है जिसे हैश (द्रुतान्वेषण) तालिका का उपयोग करके लागू किया जाता है।

राबिन–कार्प एल्गोरिथ्म (कलनविधि):

हैशिंग (द्रुतान्वेषण) के सबसे प्रसिद्ध अनुप्रयोगों में से एक रबिन–कार्प एल्गोरिथ्म (कलनविधि) है। यह मूल रूप से एक स्ट्रिंग–खोज एल्गोरिथ्म (कलनविधि) है जो एक स्ट्रिंग में पैटर्न के किसी एक समूह को खोजने के लिए हैशिंग (द्रुतान्वेषण) का उपयोग करता है। इस एल्गोरिथ्म (कलनविधि) का एक व्यावहारिक अनुप्रयोग साहित्यिक चोरी का पता लगाना है।

फाइल नाम और पथ को एक साथ जोड़नाः

हमारे स्थानीय कम्प्यूटर सिस्टम पर फाइल्स के माध्यम से आगे बढ़ने पर, हम एक फाइल के दो बहुत ही महत्वपूर्ण घटकों का निरीक्षण करते हैं, जैसे कि file_name और file_path। file_name और file_path के मध्य संपर्क को संग्रहीत करने के लिए कम्प्यूटर सिस्टम एक प्रतिचित्रण (file_name, file_path) का उपयोग करता है जिसे हैश तालिका का उपयोग करके लागू किया जाता है।

संदेशों और फाइल्स की अखंडता का सत्यापनः

सुरक्षित हैश (द्रुतान्वेषण) का एक महत्वपूर्ण अनुप्रयोग संदेश अखंडता का सत्यापन है। संदेश की तुलना करने (संदेश पर हैश **डाइजेस्ट**) की गणना पहले, और बाद में, संचरण यह निर्धारित कर सकता है कि क्या संदेश या फाइल में कोई बदलाव किया गया है।

MD5, SHA1, या SHA2 हैश (द्रुतान्वेषण) डाइजेस्ट को कभी–कभी वेबसाइट्स या फोरम पर डाउनलोड की गई फाइल्स के लिए अखंडता के सत्यापन की अनुमति देने के लिए प्रकाशित किया जाता है, जिसमें फाइल को पुनर्प्राप्त करने के लिए फाइल शेयरिंग का उपयोग प्रतिलिपि के रूप में किया जाता है। यह अभ्यास विश्वास की एक श्रृंखला स्थापित करता है जब तक कि HTTPS द्वारा प्रमाणित साइट पर हैश पोस्ट किए जाते हैं। एक क्रिप्टोग्राफिक हैश (कूटलेखीय द्रुतान्वेषण) और विश्वास की एक श्रृंखला का उपयोग करने से फाइल को दुर्भावनापूर्ण परिवर्तनों को अनदेखा करने से रोकता है। अन्य त्रुटि जैसे कि चक्रीय अतिरेक जांच कोड का पता लगाने में केवल फाइल के गैर–दुर्भावनापूर्ण परिवर्तनों के विरूद्व रोकथाम होती है।

हस्ताक्षर जनन और सत्यापनः

लगभग सभी डिजिटल (अंकीय) हस्ताक्षर योजनाओं को संदेश पर एक क्रिप्टोग्राफिक हैश (कूटलेखीय द्रुतान्वेषण) की गणना करने की आवश्यकता होती है। यह हस्ताक्षर की गणना अपेक्षाकृत छोटे, सांख्यिकीय रूप से हैश डाइजेस्ट (द्रुतान्वेषण पाचन) पर करने की अनुमति देता है। संदेश को प्रामाणिक माना जाता है यदि हस्ताक्षर सत्यापन सफल हो जाता है और संदेश पर पुनः हस्ताक्षरित हैश डाइजेस्ट (द्रुतान्वेषण पाचन) हो जाता है। तो क्रिप्टोग्राफिक हैश (कूटलेखीय द्रुतान्वेषण) की संदेश अखंडता का उपयोग सुरक्षित और कुशल डिजिटल (अंकीय) हस्ताक्षर योजनाओं को बनाने के लिए किया जाता है।

प्रूफ–ऑफ–वर्कः

प्रूफ–ऑफ–वर्क सिस्टम (या प्रोटोकॉल, या फंक्शन) डेनियल–ऑफ–सर्विस हमलों और अन्य सेवा दुर्व्यवहारों को रोकने के लिए एक आर्थिक उपाय है, जैसे कि सेवा आवश्यकताकर्ता से कुछ काम की आवश्यकता द्वारा नेटवर्क पर स्पैम, आमतौर पर इसका अर्थ कम्प्यूटर द्वारा प्रसंस्करण समय है।

इन योजनाओं की एक प्रमुख विशेषता उनकी विषमता है। कार्य को आवश्यक रूप से कठोर (लेकिन संभव) होना चाहिए, लेकिन सेवा प्रदाता के लिए परीक्षण करना आसान है। बिटकॉइन माइनिंग और हैशकैश में उपयोग की जाने वाली एक लोकप्रिय प्रणाली – बिटकॉइन में खनन को अनलॉक करने के लिए और हैशकैश में ई–मेल भेजने के लिए एक अच्छे–से–टोकन के रूप में काम करने के लिए आंशिक हैश इनवर्शन का उपयोग करता है।

प्रेषक को एक संदेश खोजने की आवश्यकता होती है जिसका हैश (द्रुतान्वेषण) मान शून्य बिट्स के साथ शुरू होता है। एक वैध संदेश प्राप्त करने के लिए प्रेषक को प्रदर्शन करने के लिए औसत कार्य हैश (द्रुतान्वेषण) **मान** में आवश्यक शून्य बिट्स की संख्या में घातांक है, जबकि प्राप्तकर्ता एकल हैश फंक्शन (द्रुतान्वेषण फलन) को निष्पादित करके संदेश की वैधता को सत्यापित कर सकता है।

उदाहरण के लिए, हैशकैश में, एक प्रेषक को एक हेडर उत्पन्न करने के लिए कहा जाता है जिसका 160 बिट SHA-1 हैश (द्रुतान्वेषण) मान में पहले 20 बिट्स शून्य के रूप में होता है। एक मान्य हेडर खोजने के लिए प्रेषक को औसतन 219 बार प्रयास करना होगा।

फाइल या डेटा पहचानकर्ताः

एक संदेश डाइजेस्ट भी एक फाइल की मजबूती से पहचान के साधन के रूप में काम कर सकता है; Git, Mercurial और Monotone सहित कई स्रोत कोड प्रबंधन प्रणाली, विशिष्ट पहचान करने के लिए विभिन्न प्रकार की सामग्री (फाइल सामग्री, निर्देशिका ट्री, वंशावली जानकारी, आदि) के SHA1 के योग का उपयोग करता है। हेडर्स–टू–पीयर फाइल शेयरिंग नेटवर्क पर फाइल्स की पहचान करने के लिए हैश का उपयोग किया जाता है।

उदाहरण के लिए, एक ed2k लिंक में, MD4-variant हैश (द्रुतान्वेषण) को फाइल आकार के साथ जोड़ा जाता है, फाइल स्रोतों का पता लगाने के लिए पर्याप्त जानकारी प्रदान करता है, फाइल डाउनलोड करता है और इसकी सामग्री की पुष्टि करता है। चुंबक लिंक एक और उदाहरण है। ऐसी फाइल हैश (द्रुतान्वेषण) अक्सर हैश (द्रुतान्वेषण) सूची या हैश ट्री (द्रुतान्वेषण वृक्ष) के शीर्ष हैश (द्रुतान्वेषण) होती है जो अतिरिक्त लाभ के लिए अनुमति देती है।

हैश फंक्शन (द्रुतान्वेषण फलन) के मुख्य अनुप्रयोगों में से एक हैश (द्रुतान्वेषण) तालिका में डेटा के तेज लुक–अप की अनुमति देना है। एक विशेष प्रकार के हैश फंक्शंस (द्रुतान्वेषण फलन) होने के कारण, क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखीय द्रुतान्वेषण फलन) इस अनुप्रयोग को भी अच्छी तरह से उधार देते हैं।

हालाँकि, मानक हैश फंक्शंस (द्रुतान्वेषण फलन) के साथ तुलना में, क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखीय द्रुतान्वेषण फलन) बहुत अधिक संगणनीय रूप से महंगे होते हैं। इस कारण से, उनका उपयोग उन संदर्भों में किया जाता है जहाँ संभावित दुर्भावनापूर्ण प्रतिभागियों द्वारा उपयोगकर्ताओं के लिए जालसाजी (अपेक्षित डेटा के समान डेटा के साथ डेटा का निर्माण) की संभावना के खिलाफ खुद को बचाने के लिए आवश्यक है।

क्रिप्टोग्राफिक हैश फंक्शंस (कूटलेखीय द्रुतान्वेषण फलन) में कई सूचना–सुरक्षा अनुप्रयोग हैं, विशेष रूप से डिजिटल (अंकीय) हस्ताक्षर, संदेश प्रमाणीकरण कोड और प्रमाणीकरण के अन्य रूपों में। उनका उपयोग साधारण हैश फंक्शंस के रूप में, हैश (द्रुतान्वेषण) तालिकाओं में डेटा को अनुक्रमित करने के लिए, फिंगरप्रिंटिंग के लिए, डुप्लिकेट डेटा (प्रतिलिपि आँकड़ा) का पता लगाने या विशिष्ट रूप से फाइल्स की पहचान करने के लिए किया जाता है, और चेकसम के रूप में आकस्मिक डेटा भ्रष्टाचार का पता लगाता है। दरअसल, सूचना–सुरक्षा संदर्भों में, क्रिप्टोग्राफिक हैश (कूटलेखीय द्रुतान्वेषण) मानों को कभी–कभी (डिजिटल) फिंगरप्रिंट, चेकसम या सिर्फ हैश मान कहा जाता है, भले ही ये सभी शब्द अलग–अलग गुणों और उद्देश्यों के साथ अधिक सामान्य कार्यों के लिए खड़े हों।

क्रिप्टोग्राफिक (कूटलेखीय) गुणों के आधार पर हैश फंक्शन (द्रुतान्वेषण फलन) के दो प्रत्यक्ष अनुप्रयोग हैं:

पासवर्ड भंडारण:

हैश फंक्शंस (द्रुतान्वेषण फलन) पासवर्ड भ्रडारण को सुरक्षा प्रदान करते हैं। पासवर्ड को स्पष्ट रूप से संग्रहीत करने के स्थान पर, ज्यादातर सभी लॉगऑन प्रक्रियाएं फाइल में पासवर्ड के हैश (द्रुतान्वेषण) मानों को संग्रहीत करती हैं। पासवर्ड फाइल में युग्म की एक तालिका होती है जो (user id, h(P)) के रूप में होती है।

एक घुसपैठिया केवल पासवर्ड की हैश (द्रुतान्वेषण) देख सकता है, भले ही उसने पासवर्ड एक्सेस किया हो। वह न तो हैश (द्रुतान्वेषण) का उपयोग करके लॉगऑन कर सकता है और न ही हैश फंक्शन (द्रुतान्वेषण फलन) से पासवर्ड प्राप्त कर सकता है क्योंकि हैश फंक्शन (द्रुतान्वेषण फलन) में पूर्व–छवि प्रतिरोध का गुण है।

डेटा अखंडता का परीक्षण:

डेटा अखंडता परीक्षण हैश फंक्शन (द्रुतान्वेषण फलन) का सबसे आम अनुप्रयोग है। इसका उपयोग डेटा फाइल्स पर चेकसम उत्पन्न करने के लिए किया जाता है। यह अनुप्रयोग उपयोगकर्ता को डेटा की शुद्धता के बारे में आश्वासन देता है।

अखंडता परीक्षण उपयोगकर्ता को मूल फाइल में किए गए किसी भी परिवर्तन का पता लगाने में सहायता करती है। हालाँकि, यह मौलिकता के बारे में कोई आश्वासन नहीं देता है। हमलावर, फाइल डेटा को संशोधित करने के बजाय, पूरी फाइल को बदल सकता है और सभी नए हैश (द्रुतान्वेषण) की गणना कर सकता है और प्राप्तकर्त्ता को भेज सकता है। यह अखंडता परीक्षण अनुप्रयोग केवल तभी उपयोगी है जब उपयोगकर्ता फाइल की मौलिकता के बारे में सुनिश्चित हो।

इन गुणों के साथ फलन को विभिन्न प्रयोजनों के लिए हैश फंक्शन (द्रुतान्वेषण फलन) के रूप में उपयोग किया जाता है, न केवल क्रिप्टोग्राफी (कूटलेखन) में। व्यावहारिक अनुप्रयोगों में संदेश अखंडता परीक्षण, डिजिटल (अंकीय) हस्ताक्षर, प्रमाणीकरण और विभिन्न सूचना सुरक्षा अनुप्रयोग सम्मिलित हैं।

एक हैश फंक्शन (द्रुतान्वेषण फलन) इनपुट (निवेश) के रूप में किसी भी लंबाई की एक स्ट्रिंग लेता है और एक निश्चित लंबाई की स्ट्रिंग उत्पन्न करता है जो प्रदान किए गए डेटा के लिए हस्ताक्षर के रूप में कार्य करता है।

इस प्रकार, हैश (द्रुतान्वेषण) मान जानने वाला व्यक्ति मूल संदेश को जानने में असमर्थ होता है, लेकिन केवल वह व्यक्ति जो मूल संदेश जानता है वह हैश (द्रुतान्वेषण) मान को उस संदेश से बनाया जा सकता है। एक क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखीय द्रुतान्वेषण फलन) को एक यादृच्छिक फलन की तरह जितना संभव हो उतना व्यवहार करना चाहिए, जबकि निर्धारक और कुशलतापूर्वक संगणनीय हो। एक क्रिप्टोग्राफिक हैश फंक्शन (कूटलेखीय द्रुतान्वेषण फलन) को क्रिप्टोग्राफिक (कूटलेखीय) दृष्टिकोण से असुरक्षित माना जाता है, यदि निम्न में से कोई भी संगणनीय रूप से संभव है:

1. एक (पहले अनदेखी) संदेश खोजना जो किसी दिए गए हैश (द्रुतान्वेषण) मानों से मेल खाता है।
2. टकराव ढूँढना, जिसमें दो अलग–अलग संदेशों में समान हैश (द्रुतान्वेषण) मान होता है।

एक हमलावर जो उपरोक्त गणनाओं में से किसी को भी पा सकता है, उन्हें एक अनधिकृत के साथ एक अधिकृत संदेश को प्रतिस्थापित करने के लिए उपयोग कर सकता है।

आदर्श रूप से, दो अलग–अलग संदेशों को ढूंढना असंभव होना चाहिए जिनकी डाइजेस्ट (हैश मान) समान हैं। इसके अतिरिक्त, कोई भी यह नहीं चाहेगा कि एक हमलावर अपने डाइजेस्ट (हैश मान) से एक संदेश के बारे में उपयोगी कुछ भी सीख सके। बेशक हमलावर कम से कम एक जानकारी को सीखता है, जिसके द्वारा हमलावर यह पहचान सकता है कि क्या फिर से वही संदेश आया था।

विभिन्न मानकों और अनुप्रयोगों में, दो सबसे अधिक उपयोग किए जाने वाले हैश फंक्शन MD5 और SHA-1 हैं।

2005 में, सुरक्षा दोषों की पहचान यह दिखाते हुए की गई कि एक संभावित गणितीय कमजोरी मौजूद हो सकती है, जैसे हमले, और एक मजबूत हैश फंक्शन (द्रुतान्वेषण फलन) की सिफारिश करना।

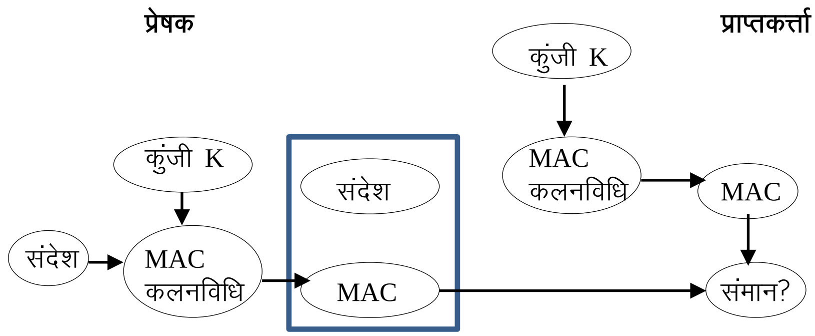
2007 में नेशनल इंस्टीट्यूट ऑफ स्टैंडर्ड्स एंड टेक्नोलॉजी ने एक हैश फंक्शन (द्रुतान्वेषण फलन) को अभिकल्पित करने के लिए एक प्रतियोगिता की घोषणा की, जिसे SHA-3 नाम दिया जाएगा और एक FIPS मानक का विषय होगा।

6.7 संदेश प्रमाणीकरण:

पूर्व अनुच्छेदों में, हमने डेटा अखंडता खतरों और हैशिंग (द्रुतान्वेषण) तकनीक के उपयोग पर चर्चा की ताकि यह पता लगाया जा सके कि डेटा पर कोई संशोधन हमले हुए हैं या नहीं। एक अन्य प्रकार का खतरा जो डेटा के लिए मौजूद है, वह संदेश प्रमाणीकरण की कमी है। इस धमकी में, उपयोगकर्ता संदेश के प्रवर्तक के बारे में निश्चित नहीं है। गुप्त प्रमाणीकरण तकनीक का उपयोग करके संदेश प्रमाणीकरण प्रदान किया जा सकता है जो एन्क्रिप्शन (कूट प्रक्रिया) की दशा में गुप्त कुंजी का उपयोग करता है।

संदेश प्रमाणीकरण कोड (MAC):

MAC एल्गोरिथ्म (कलनविधि) संदेश प्रमाणीकरण प्रदान करने के लिए एक सममित कुंजी क्रिप्टोग्राफिक (कूटलेखीय) तकनीक है। MAC प्रक्रिया की स्थापना के लिए, प्रेषक और प्राप्तकर्त्ता एक सममित कुंजी K साझा करते हैं। आवश्यक रूप से, MAC एक एन्क्रिप्टेड चेकसम (कूटित जाँच योग) है जो अंतर्निहित संदेश पर उत्पन्न होता है जो संदेश प्रमाणीकरण सुनिश्चित करने के लिए एक संदेश के साथ भेजा जाता है। प्रमाणीकरण के लिए MAC का उपयोग करने की प्रक्रिया को निम्न चित्र में दर्शाया गया है –



(चित्र क्र0 6.6)

अब पूरी प्रक्रिया को विस्तार से समझते हैं –

प्रेषक कुछ सार्वजनिक रूप से ज्ञात MAC एल्गोरिथ्म (कलनविधि) का उपयोग करता है, संदेश और गुप्त कुंजी K को इनपुट करता है और एक MAC मान उत्पन्न करता है। हैश (द्रुतान्वेषण) के समान, MAC फलन भी एक निश्चित लंबाई आउटपुट में एक वांछित लंबा इनपुट (निवेश) को संपीड़ित करता है। हैश (द्रुतान्वेषण) और MAC के मध्य मुख्य अंतर यह है कि MAC संपीड़न के दौरान गुप्त कुंजी का उपयोग करता है।

MAC के साथ संदेश भेजने वाले को अग्रेषित करता है। यहाँ, हम मानते हैं कि संदेश स्पष्ट में भेजा गया है, क्योंकि संदेश मूल प्रमाणीकरण प्रदान करने से संबंधित हैं, गोपनीयता नहीं। यदि गोपनीयता की आवश्यकता है तो संदेश को एन्क्रिप्शन (कूट प्रक्रिया) की आवश्यकता है।

संदेश और MAC की प्राप्ति पर, प्राप्तकर्त्ता प्राप्त संदेश और MAC एल्गोरिथ्म में साझा गुप्त कुंजी K और MAC मान को फिर से गणना करता है।

प्राप्तकर्त्ता अब प्रेषक से प्राप्त MAC के साथ हौसले से गणना किए गए MAC की समानता का परीक्षण करता है। यदि वे सुमेलित होते हैं, तो प्राप्तकर्त्ता संदेश को स्वीकार करता है और स्वयं को आश्वस्त करता है कि संदेश इच्छित प्रेषक द्वारा भेजा गया है।

यदि गणना किए गए MAC प्रेषक द्वारा भेजे गए MAC से सुमेलित नहीं होते हैं, तो प्राप्तकर्त्ता यह निर्धारित नहीं कर सकता है कि क्या यह संदेश है जिसे बदल दिया गया है या यह मूल है जिसे गलत ठहराया गया है। निम्न–रेखा के रूप में, एक प्राप्तकर्त्ता सुरक्षित रूप से मानता है कि संदेश वास्तविक नहीं है।

MAC की सीमाएँ:

MAC की दो प्रमुख सीमाएं हैं, दोनों इसके संचालन की सममित प्रकृति के कारण:

साझा रहस्य की स्थापना:

यह पूर्व–निश्चित वैध उपयोगकर्ताओं के बीच संदेश प्रमाणीकरण प्रदान कर सकता है, जिनके पास साझा कुंजी है। इसके लिए MAC के उपयोग से पहले साझा रहस्य की स्थापना की आवश्यकता होती है।

गैर–परित्याग प्रदान करने में असमर्थता:

गैर–परित्याग यह आश्वासन है कि एक संदेश प्रवर्तक किसी भी पहले भेजे गए संदेशों और प्रतिबद्धताओं या कार्यों से इनकार नहीं कर सकता है। MAC तकनीक एक गैर–परित्याग सेवा प्रदान नहीं करता है। यदि संदेश भेजने पर प्रेषक और प्राप्तकर्त्ता विवाद में सम्मिलित होते हैं, तो MAC इस बात का प्रमाण नहीं दे सकते कि संदेश भेजने वाले ने वास्तव में भेजा था।

यद्यपि कोई भी तीसरा पक्ष MAC की गणना नहीं कर सकता है, फिर भी प्रेषक संदेश भेजने से मना कर सकता है और दावा कर सकता है कि प्राप्तकर्त्ता ने इसे नकली बनाया है, क्योंकि यह निर्धारित करना असंभव है कि दोनों पक्षों में से किसने MAC की गणना की।

6.8 चेकसम (जाँच योग):

एक चेकसम (जाँच योग) कुछ डेटा के साथ जानकारी का एक अतिरिक्त भाग भेजने का एक सरल तरीका है जिसका उपयोग यह सुनिश्चित करने के लिए किया जा सकता है कि डेटा दोनों पक्षों पर समान है। अन्य शब्दों में, यह किसी को फोन पर हमसे एक नंबर दोहराने के लिए कहने जैसा है। जानकारी को दोहराते समय कम संख्या के लिए ठीक काम करता है, अगर हमारे पास बड़ी मात्रा में डेटा है तो यह थोड़ा परेशान कर सकता है। उदाहरण के लिए, यदि कोई व्यक्ति किसी अन्य व्यक्ति को फोन पर कुछ मान पढ़ कर बता रहा है, और दूसरा व्यक्ति उन्हें एक्सेल में टाइप कर रहा है। इसके पश्चात् दोनों आंकड़ों का मेल करते हैं। इस कार्य में लंबा समय लगेगा। इसके स्थान पर, यदि योग का आदान प्रदान किया जाये और वह मेल खाता हो, तो निम्न दो चीजों में से एक हुआ:

1. मौखिक रूप से संख्याओं को सफलतापूर्वक स्थानांतरित कर दिया गया है।
2. कुछ गलतियाँ हुईं जो एक दूसरे को पूरी तरह से रद्द कर देती हैं।

चूंकि संख्या की एक बड़ी सूची के साथ काम करते समय दूसरे विकल्प की संभावना बहुत कम है, इसलिए हम यह मान सकते हैं कि हमने कोई गलती नहीं की है।

कम्प्यूटर एक समान तरीके से चेकसम (जाँच येाग) का उपयोग करते हैं। मॉडेम के दिनों में, कम्प्यूटर एक 8 बिट बाइट भेजते हैं, जहां अंतिम बिट एक चेकसम (जाँच येाग) होता था। इसलिए, कम्प्यूटर एक द्विआधारी संदेश भेज सकता है जो इस तरह दिखता थाः

01101010

पहले 7 बिट्स में डेटा सम्मिलित थाः 0110101। अंतिम बिट चेकसम (जाँच येाग) का उपयोग यह बताने के लिए किया गया था कि क्या डेटा में सम या विषम संख्याएँ मौजूद थीं। इस दशा में हम कहने के लिए 0 का उपयोग कर रहे हैं कि यहाँ तक कि संख्या भी हैं। यदि प्राप्त करने वाले कम्प्यूटर को एक बाइट मिलता है जहाँ बिट्स की संख्या और चेकसम थोड़ा असहमत होता है, तो वह उस डेटा को फिर से भेजने के लिए कहेगा।

इस प्रकार का दृष्टिकोण आकस्मिक त्रुटियों को कम करता है। हालाँकि, यह किसी को जानबूझकर डेटा बदलने से रोकने की दिशा में कुछ नहीं करता है। यदि हम डेटा का मार्ग बदलना चाहते हैं, तो चेकसम (जाँच येाग) बिट्स को फ्लिप करना सरल होगा, जो हम डेटा में भेजना चाहते थे। हमें एक चेकसम (जाँच येाग) प्रकार मान उत्पन्न करने का एक विधि चाहिए जो नकली के लिए कठिन हो।

अभ्यास

1. क्रिप्टोग्राफी हैश फंक्शन (कूटलेखन द्रुतान्वेषण फलन) से क्या समझते हैं?
2. हैश फंक्शन (द्रुतान्वेषण फलन) की विशेषतायें लिखिए।
3. हैश फंक्शन (द्रुतान्वेषण फलन) के प्रगुण बताइए।
4. हैशिंग एल्गोरिथम (द्रुतान्वेषण कलन विधि) की अभिकल्पना को समझाइए।
5. प्रसिद्व हैश फंक्शन (द्रुतान्वेषण फलन) कौन–कौन से हैं?
6. मैसेज डाइजेस्ट (संदेश संग्रह) पर टिप्पणी लिखिए।
7. सुरक्षित हैश फंक्शन (द्रुतान्वेषण फलन) क्या है?
8. RIPEMD से क्या समझते हैं?
9. व्हर्लपूल क्या है?
10. हैश फंक्शन (द्रुतान्वेषण फलन) के अनुप्रयोग लिखिए।
11. संदेश प्रमाणीकरण को समझाइए।
12. चेकसम (जाँच योग) से क्या समझते हैं?

अध्याय – 7

डिजिटल सिग्नेचर
(अंकीय हस्ताक्षर)

7.1 क्रिप्टोग्राफी डिजिटल सिग्नेचर (कूटलेखन अंकीय हस्ताक्षर):

डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) या हस्ताक्षर संदेश प्रमाणीकरण की सबसे पुरानी सार्वजनिक–कुंजी है। भौतिक दुनिया में, हस्तलिखित या टंकित किए गए संदेशों पर हस्तलिखित हस्ताक्षर का उपयोग करना आम है। वे संदेश को हस्ताक्षरकर्ता को बांधने के लिए उपयोग किए जाते हैं।

इसी प्रकार, डिजिटल (अंकीय) हस्ताक्षर एक ऐसी तकनीक है जो किसी व्यक्ति/इकाई को डिजिटल डेटा (अंकीय आँकड़ों) से बांधती है। इस बंधन को प्राप्तकर्त्ता और साथ ही किसी भी तीसरे पक्ष द्वारा स्वतंत्र रूप से सत्यापित किया जा सकता है।

डिजिटल (अंकीय) हस्ताक्षर एक क्रिप्टोग्राफिक (कूटलेखीय) मान है जो डेटा और एक गुप्त कुंजी जिसे केवल हस्ताक्षरकर्ता द्वारा जाना जाता है, से गणना की जाती है। वास्तविक दुनिया में, संदेश के प्राप्तकर्त्ता को आश्वासन की आवश्यकता होती है कि संदेश प्रेषक का है और उसे उस संदेश की उत्पत्ति को निरस्त करने में सक्षम नहीं होना चाहिए। व्यावसायिक अनुप्रयोगों में यह आवश्यकता बहुत महत्वपूर्ण है, क्योंकि विनिमय किए गए डेटा पर विवाद की संभावना बहुत अधिक है।

एक डिजिटल (अंकीय) हस्ताक्षर एक गणितीय तकनीक है जिसका उपयोग किसी संदेश, सॉफ्टवेयर या डिजिटल (अंकीय) दस्तावेज की प्रामाणिकता और अखंडता को मान्य करने के लिए किया जाता है। हस्तलिखित हस्ताक्षर या मोहरबंद मुहर के डिजिटल (अंकीय) समकक्ष, एक डिजिटल (अंकीय) हस्ताक्षर कहीं अधिक अंतर्निहित सुरक्षा प्रदान करता है, और इसका उद्देश्य डिजिटल (अंकीय) संचार में छेड़छाड़ और प्रतिरूपण की समस्या को हल करना है।

डिजिटल (अंकीय) हस्ताक्षर एक इलेक्ट्रॉनिक दस्तावेज, लेनदेन या संदेश की उत्पत्ति, पहचान और स्थिति के साक्ष्य के अतिरिक्त आश्वासन प्रदान कर सकते हैं और हस्ताक्षरकर्ता द्वारा सूचित सहमति को स्वीकार कर सकते हैं।

संयुक्त राज्य अमेरिका सहित कई देशों में, डिजिटल (अंकीय) हस्ताक्षर को पारंपरिक दस्तावेज हस्ताक्षर के समान कानूनी रूप से बाध्यकारी माना जाता है। यूनाइटेड स्टेट्स गवर्नमेंट पब्लिशिंग ऑफिस बजट, सार्वजनिक और निजी कानूनों के इलेक्ट्रॉनिक संस्करण और डिजिटल (अंकीय) हस्ताक्षर के साथ कांग्रेस के बिल प्रकाशित करता है।

डिजिटल (अंकीय) हस्ताक्षर कैसे काम करते हैं?

डिजिटल (अंकीय) हस्ताक्षर सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) पर आधारित होते हैं, जिन्हें असममित क्रिप्टोग्राफी (कूटलेखन) भी कहा जाता है। सार्वजनिक कुंजी एल्गोरिथ्म (कलनविधि) का उपयोग करना, जैसे कि RSA, दो कुंजी उत्पन्न कर सकता है जो गणितीय रूप से जुड़े हुए हैंः एक व्यक्तिगत और एक सार्वजनिक।

डिजिटल (अंकीय) हस्ताक्षर काम करते हैं क्योंकि सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) दो पारस्परिक रूप से प्रमाणीकरण क्रिप्टोग्राफिक (कूटलेखीय) कुंजियों पर निर्भर करती है। जो व्यक्ति डिजिटल (अंकीय) हस्ताक्षर बना रहा है, वह हस्ताक्षर–संबंधी डेटा को एन्क्रिप्ट (कूटित) करने के लिए अपनी व्यक्तिगत कुंजी का उपयोग करता है, उस डेटा को डिक्रिप्ट (अकूटित) करने का एकमात्र तरीका है हस्ताक्षरकर्ता की सार्वजनिक कुंजी। इस तरह डिजिटल (अंकीय) हस्ताक्षर प्रमाणित होते हैं।

डिजिटल (अंकीय) हस्ताक्षर तकनीक में सभी पक्षों को यह विश्वास करने की आवश्यकता है कि हस्ताक्षर बनाने वाला व्यक्ति अपनी व्यक्तिगत कुंजी को गुप्त रखने में सक्षम है। यदि किसी और के पास हस्ताक्षरकर्ता की व्यक्तिगत कुंजी तक पहुँच है, तो वह पक्ष निजी कुंजी धारक के नाम पर कपटपूर्ण डिजिटल (अंकीय) हस्ताक्षर बना सकती है।

डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) कैसे बनाये?

एक डिजिटल (अंकीय) हस्ताक्षर बनाने के लिए, सॉफ्टवेयर पर हस्ताक्षर करना, जैसे कि ईमेल प्रोग्राम पर हस्ताक्षर किए जाने वाले इलेक्ट्रॉनिक डेटा का एक तरफा हैश बनाता है।

व्यक्तिगत कुंजी तब हैश (द्रुतान्वेषण) को एन्क्रिप्ट (कूटित) करने के लिए उपयोग की जाती है। एन्क्रिप्टेड हैश (कूटित द्रुतान्वेषण) अन्य जानकारी के साथ, जैसे हैशिंग एल्गोरिथ्म (द्रुतान्वेषण कलनविधि), डिजिटल (अंकीय) हस्ताक्षर है। पूरे संदेश या दस्तावेज के स्थान पर हैश (द्रुतान्वेषण) को एन्क्रिप्ट (कूटित) करने का कारण यह है कि एक हैश फंक्शन (द्रुतान्वेषण फलन) एक वांछित इनपुट (निवेश) को नियत लंबाई मान में बदल सकता है, जो आमतौर पर बहुत छोटा होता है। यह समय बचाता है क्योंकि हैशिंग (द्रुतान्वेषण) हस्ताक्षर करने की तुलना में बहुत तेज है।

हैश (द्रुतान्वेषण) का मान हैशेड (द्रुतान्वेषण) डेटा के लिए अद्वितीय है। डेटा में कोई भी परिवर्तन, यहाँ तक कि किसी एकल कैरेक्टर (संप्रतीक) में परिवर्तन, एक अलग मूल्य में परिणाम देगा। यह विशेषता अन्य लोगों को हैश (द्रुतान्वेषण) को डिक्रिप्ट (अकूटित) करने के लिए हस्ताक्षरकर्ता की सार्वजनिक कुंजी का उपयोग करके डेटा की अखंडता को मान्य करने में सक्षम बनाती है।

यदि डिक्रिप्टेड हैश (अकूटित द्रुतान्वेषण) उसी डेटा के दूसरे गणना किए गए हैश (द्रुतान्वेषण) से मेल खाता है, तो यह साबित होता है कि हस्ताक्षर किए जाने के बाद से डेटा नहीं बदला है। यदि दो हैश (द्रुतान्वेषण) मेल नहीं खाते हैं, तो डेटा के साथ किसी तरह से छेड़छाड़ की गई है। अखंडता या हस्ताक्षर एक निजी कुंजी के साथ बनाया गया था जो हस्ताक्षरकर्ता प्रमाणीकरण द्वारा प्रस्तुत सार्वजनिक कुंजी के अनुरूप नहीं है।

एक डिजिटल (अंकीय) हस्ताक्षर का उपयोग किसी भी प्रकार के संदेश के साथ किया जा सकता है, चाहे यह एन्क्रिप्ट (कूटित) किया गया हो या नहीं। केवल इसलिए प्राप्तकर्त्ता को प्रेषक की पहचान सुनिश्चित हो सकती है और यह संदेश बरकरार रहा। डिजिटल (अंकीय) हस्ताक्षर हस्ताक्षरकर्ता के लिए कुछ हस्ताक्षर करने से इनकार करना मुश्किल बनाते हैं, यह मानते हुए कि उनकी व्यक्तिगत कुंजी से समझौता नहीं किया गया है। चूंकि डिजिटल (अंकीय) हस्ताक्षर दस्तावेज और हस्ताक्षरकर्ता दोनों के लिए अद्वितीय है और यह उन्हें एक साथ बांधता है, अतः इस गुण को अ–परित्याग कहा जाता है।

डिजिटल (अंकीय) हस्ताक्षर डिजिटल प्रमाणपत्रों के साथ भ्रमित नहीं होने चाहिए। एक डिजिटल (अंकीय) प्रमाणपत्र, एक इलेक्ट्रॉनिक दस्तावेज जिसमें जारी करने वाले प्रमाणपत्र प्राधिकारी के डिजिटल (अंकीय) हस्ताक्षर होते हैं, एक सार्वजनिक कुंजी को एक पहचान के साथ बांधता है और यह सत्यापित करने के लिए उपयोग किया जा सकता है कि सार्वजनिक कुंजी किसी विशेष व्यक्ति या संस्था से संबंधित है।

अधिकांश आधुनिक ईमेल प्रोग्राम डिजिटल (अंकीय) हस्ताक्षर और डिजिटल (अंकीय) प्रमाणपत्र के उपयोग का समर्थन करते हैं, जिससे किसी भी आउटगोइंग ईमेल पर हस्ताक्षर करना आसान हो जाता है और आने वाले संदेशों को डिजिटल (अंकीय) रूप से हस्ताक्षरित किया जा सकता है। डिजिटल (अंकीय) हस्ताक्षर का उपयोग बड़े पैमाने पर इंटरनेट पर आयोजित संचार और लेनदेन की प्रामाणिकता, डेटा अखंडता और गैर–प्रसार के प्रमाण प्रदान करने के लिए किया जाता है।

डिजिटल (अंकीय) हस्ताक्षर बनाम इलेक्ट्रॉनिक हस्ताक्षरः

डिजिटल (अंकीय) हस्ताक्षर एक तकनीकी शब्द है, एक क्रिप्टोग्राफिक (कूटलेखीय) प्रक्रिया के परिणाम को परिभाषित करते हुए जिसका उपयोग डेटा के एक अनुक्रम को प्रमाणित करने के लिए किया जा सकता है, इलेक्ट्रॉनिक हस्ताक्षर या ई–हस्ताक्षर एक कानूनी शब्द है जिसे विधायी रूप से परिभाषित किया गया है।

उदाहरण के लिए, संयुक्त राज्य अमेरिका में, शब्द को ग्लोबल एंड नेशनल कॉमर्स एक्ट में इलेक्ट्रॉनिक हस्ताक्षरों में परिभाषित किया गया था, जिसे 2000 में पारित किया गया था, जिसका अर्थ है एक इलेक्ट्रॉनिक ध्वनि, प्रतीक या प्रक्रिया, जो अनुबंध या अन्य रिकॉर्ड के साथ या तार्किक रूप से जुड़ा हुआ है। और रिकॉर्ड पर हस्ताक्षर करने के इरादे से किसी व्यक्ति द्वारा निष्पादित या अपनाया गया।

इसका अर्थ है कि एक डिजिटल (अंकीय) हस्ताक्षर जिसे इलेक्ट्रॉनिक रूप में डिजिटल (अंकीय) रूप से व्यक्त किया जा सकता है और एक रिकॉर्ड के प्रतिनिधित्व के साथ जुड़ा हुआ है एक प्रकार का इलेक्ट्रॉनिक हस्ताक्षर हो सकता है। आमतौर पर, हालांकि, इलेक्ट्रॉनिक हस्ताक्षर उतना ही सरल हो सकता है, जितना कि हस्ताक्षरकर्ता का नाम वेबपेज पर एक फॉर्म में दर्ज किया जा रहा है। मान्य माना जाने के लिए, इलेक्ट्रॉनिक हस्ताक्षर योजनाओं में निम्न तीन चीजें शामिल होनी चाहिएः

- हस्ताक्षर करने वाली संस्था की पहचान को सत्यापित करने की एक विधि।

- यह सत्यापित करने की एक विधि है कि हस्ताक्षर करने वाली संस्था को दस्तावेज पर हस्ताक्षर किए जाने की पुष्टि करना है।
- यह सत्यापित करने की एक विधि है कि इलेक्ट्रॉनिक हस्ताक्षर वास्तव में हस्ताक्षरित दस्तावेज के साथ जुड़ा हुआ है।

प्रमाणित डिजिटल (अंकीय) हस्ताक्षर क्रिप्टोग्राफिक (कूटलेखीय) प्रमाण प्रदान करते हैं कि एक दस्तावेज पर हस्ताक्षरित संस्था द्वारा हस्ताक्षरित किया गया था और दस्तावेज को बदला नहीं दिया गया है, सभी इलेक्ट्रॉनिक हस्ताक्षर समान गारंटी प्रदान नहीं कर सकते हैं।

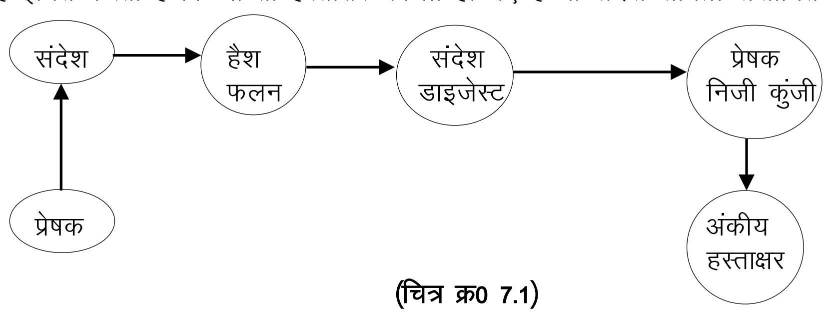
प्रमाणीकरण की कोई भी प्रक्रिया दो पक्षों को किसी तीसरे पक्ष के विरुद्ध सुरक्षा प्रदान करती है। हालांकि, यह प्रक्रिया एक दूसरे के खिलाफ पक्षों की रक्षा नहीं करती है। इसका अर्थ यह है कि उन स्थितियों में जहाँ प्रेषक और प्राप्तकर्ता के मध्य पूर्ण विश्वास नहीं है, प्रमाणीकरण से अधिक कुछ आवश्यक है। डिजिटल (अंकीय) हस्ताक्षर का उपयोग करके इस समस्या को हल किया जा सकता है। एक डिजिटल (अंकीय) हस्ताक्षर हस्तलिखित हस्ताक्षर के अनुरूप है और हस्ताक्षर के लेखक, तिथि और समय की पुष्टि करता है। हस्ताक्षर, हस्ताक्षर के समय सामग्री को प्रमाणित करने में भी सक्षम होना चाहिए। डिजिटल (अंकीय) हस्ताक्षर की मुख्य आवश्यकताएँ निम्न हैं:

- यह प्रेषक के लिए अद्वितीय है।
- इसे पहचानने योग्य और सत्यापन योग्य होना चाहिए।

डिजिटल (अंकीय) हस्ताक्षरों के लिए कई तरह के दृष्टिकोण हैं, जो मोटे तौर पर दो श्रेणियों में आते हैं– प्रत्यक्ष और मध्यस्थ।

प्रत्यक्ष डिजिटल (अंकीय) हस्ताक्षरः

प्रेषक की व्यक्तिगत कुंजी के साथ पूरे संदेश को एन्क्रिप्ट (कूटित) करके या प्रेषक की व्यक्तिगत कुंजी के साथ संदेश के हैश (द्रुतान्वेषण) मान को एन्क्रिप्ट (कूटित) करके एक प्रत्यक्ष डिजिटल (अंकीय) हस्ताक्षर बनाया जा सकता है। निम्नलिखित चित्र डिजिटल (अंकीय) हस्ताक्षर बनाने की प्रक्रिया को बताता है। आउटपुट (निर्गत) को डिजिटल (अंकीय) हस्ताक्षर कहा जाता है और यह संदेश से जुड़ा होता है। हस्ताक्षर को सत्यापित करने के लिए, प्राप्तकर्ता संदेश, हस्ताक्षर और प्रेषक की सार्वजनिक कुंजी को शामिल करता है। यदि परिणाम अनुरूप है, तो हस्ताक्षर को प्रामाणिक माना जाता है। अन्यथा, हस्ताक्षर को नकली माना जाता है या संदेश के साथ छेड़छाड़ की गई है। ऐसा इसलिए है क्योंकि गणना किया गया मान हस्ताक्षर और संदेश की सामग्री पर आधारित है। डिजिटल (अंकीय) हस्ताक्षर या संदेश की सामग्री के मानों में कोई भी परिवर्तन गणना मान और प्राप्त मान के मध्य एक असुमेलन का परिणाम है। यह इंगित करता है कि या तो हस्ताक्षर नकली हो गए हैं या संदेश सामग्री संशोधित हो गई है।



(चित्र क्र0 7.1)

इसके अतिरिक्त पूरे संदेश को एन्क्रिप्ट (कूटित) करना और डिजिटल (अंकीय) हस्ताक्षर गोपनीयता प्रदान कर सकते हैं। संदेश में डिजिटल (अंकीय) हस्ताक्षर जोड़ना और फिर पूरे संदेश को एन्क्रिप्ट (कूटित) करना महत्वपूर्ण है। पहले संदेश को एन्क्रिप्ट (कूटित) करने के स्थान पर, डिजिटल (अंकीय) हस्ताक्षर की गणना की जानी चाहिए और हस्ताक्षर में जोड़ा जाना चाहिए। यदि उत्तरार्द्ध दृष्टिकोण लिया जाता है, तो तीसरे पक्ष को संदेश पढ़ने के लिए डिक्रिप्शन (अकूट प्रक्रिया) विधि का उपयोग करने की आवश्यकता होती है। अन्यथा, भविष्य के विवादों के समाधान के लिए केवल सादे और डिजिटल (अंकीय) हस्ताक्षर को रखा जा सकता है।

प्रत्यक्ष डिजिटल (अंकीय) हस्ताक्षर योजना में एक कमी है – पूरी योजना प्रेषक की व्यक्तिगत कुंजी की वैधता पर निर्भर करती है। यदि प्रेषक उस जिम्मेदारी को अस्वीकार करता है जो उसने संदेश भेजा है और दावा करता है कि व्यक्तिगत कुंजी खो गई है या समझौता किया गया है, तो किसी को हस्ताक्षर को जाली करना होगा।

स्वेच्छ डिजिटल (अंकीय) हस्ताक्षरः

प्रत्यक्ष डिजिटल (अंकीय) हस्ताक्षर में सामने आई अ–परित्याग की समस्या को दूर करने के लिए स्वेच्छ डिजिटल (अंकीय) हस्ताक्षर योजना का उपयोग किया जाता है। इस योजना में, प्रेषक के प्रत्येक हस्ताक्षरित संदेश, जो प्राप्तकर्ता को भेजा गया है, पहले एक मध्यस्थ के पास जाता है जो हस्ताक्षर की उत्पत्ति और सामग्री के बारे में परीक्षण करता है। संदेश को दिनांकित किया जाता है और प्राप्तकर्ता को भेज दिया जाता है। मध्यस्थ की उपस्थिति हस्ताक्षर को प्रेषित करने वाले प्रेषक की समस्या को हल करती है। उदाहरण के लिए, जब X, Y को एक डिजिटली (अंकीय) हस्ताक्षरित संदेश भेजता है, तो एक मध्यस्थ पहले X के हस्ताक्षर की पुष्टि करता है। हस्ताक्षर को मान्य किए जाने के बाद, संदेश तब Y को सत्यापन की तारीख और नोटिस के साथ भेजा जाता है कि हस्ताक्षर X का है।

डिजिटल (अंकीय) हस्ताक्षर बनाने में निम्नलिखित चरण हैं:

1. मैसेज डाइजेस्ट (संदेश पाचन) को संदेश पर हैश फंक्शन (द्रुतान्वेषण फलन) लागू करके पूर्ण किया जाता है और फिर डिजिटल (अंकीय) हस्ताक्षर बनाने के लिए प्रेषक की व्यक्तिगत कुंजी का उपयोग करके मैसेज डाइजेस्ट (संदेश पाचन) को एन्क्रिप्ट (कूटित) किया जाता है। (डिजिटल हस्ताक्षर = एन्क्रिप्शन (प्रेषक, संदेश डाइजेस्ट की व्यक्तिगत कुंजी) और संदेश डाइजेस्ट = संदेश डाइजेस्ट एल्गोरिथम (संदेश)।
2. डिजिटल हस्ताक्षर तब संदेश के साथ प्रेषित किया जाता है। (संदेश + डिजिटल हस्ताक्षर प्रेषित किया जाता है)
3. प्राप्तकर्ता प्रेषक की सार्वजनिक कुंजी का उपयोग करके डिजिटल (अंकीय) हस्ताक्षर को डिक्रिप्ट (अकूटित) करता है। (यह प्रामाणिकता का आश्वासन देता है, क्योंकि केवल प्रेषक के पास अपनी व्यक्तिगत कुंजी है इसलिए केवल प्रेषक अपनी व्यक्तिगत कुंजी का उपयोग करके एन्क्रिप्ट (कूटित) कर सकता है जिसे इस प्रकार प्रेषक की सार्वजनिक कुंजी द्वारा डिक्रिप्ट (अकूटित) किया जा सकता है)।
4. प्राप्तकर्ता के पास अब मैसेज डाइजेस्ट (संदेश पाचन) है।
5. प्राप्तकर्ता संदेश से मैसेज डाइजेस्ट (संदेश पाचन) की गणना कर सकता है (वास्तविक संदेश डिजिटल हस्ताक्षर के साथ भेजा जाता है)।
6. रिसीवर द्वारा गणना की गई मैसेज डाइजेस्ट (संदेश पाचन) और मैसेज डाइजेस्ट (संदेश पाचन) (डिजिटल सिग्नेचर पर डिक्रिप्शन द्वारा मिला) अखंडता सुनिश्चित करने के लिए समान होना चाहिए।

मैसेज डाइजेस्ट (संदेश पाचन) को एक तरफा हैश फंक्शन (द्रुतान्वेषण फलन), यानी एक हैश फंक्शन (द्रुतान्वेषण फलन) का उपयोग करके गणना की जाती है जिसमें हैश (द्रुतान्वेषण) मान की गणना आसान है, लेकिन एक हैश (द्रुतान्वेषण) मान से गणना करना अत्यंत कठिन है।

7.2 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) का प्रारूप :

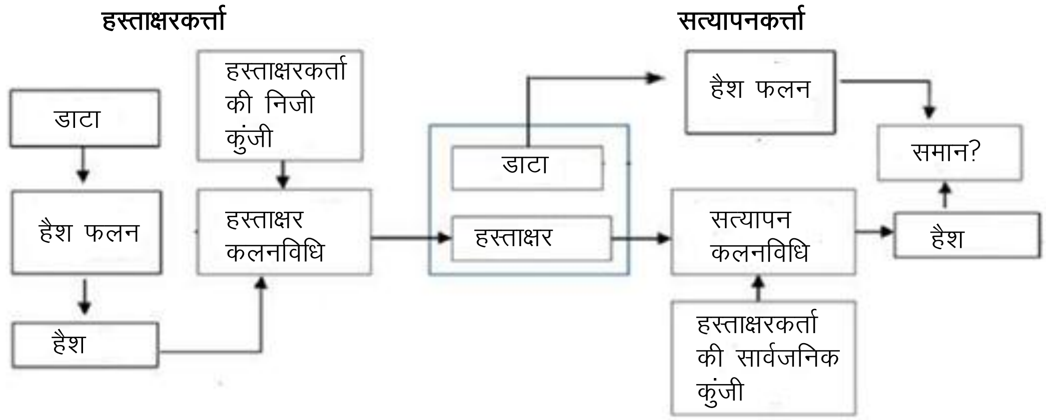
जैसा कि पहले उल्लेख किया गया है, डिजिटल (अंकीय) हस्ताक्षर योजना सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) पर आधारित है।

निम्नलिखित बिंदु पूरी प्रक्रिया को विस्तार से बताते हैं –

- इस योजना को अपनाने वाले प्रत्येक व्यक्ति के पास एक सार्वजनिक–व्यक्तिगत कुंजी युग्म होता है।
- आमतौर पर, एन्क्रिप्शन/डिक्रिप्शन (कूट प्रक्रिया/अकूट प्रक्रिया) और हस्ताक्षर/सत्यापन के लिए उपयोग किए जाने वाले कुंजी युग्म पृथक–पृथक होते हैं। हस्ताक्षर करने के लिए उपयोग की जाने वाली व्यक्तिगत कुंजी को हस्ताक्षर कुंजी और सत्यापन कुंजी के रूप में सार्वजनिक कुंजी के रूप में संदर्भित किया जाता है।
- हस्ताक्षरकर्ता हैश फंक्शन (द्रुतान्वेषण फलन) को डेटा फीड करता है और डेटा का हैश (द्रुतान्वेषण) उत्पन्न करता है।

- हैश (द्रुतान्वेषण) मान और हस्ताक्षर कुंजी तब हस्ताक्षर एल्गोरिथ्म (कलनविधि) को फेड (fed) किया जाता है जो दिए गए हैश (द्रुतान्वेषण) पर डिजिटल (अंकीय) हस्ताक्षर का उत्पादन करता है। हस्ताक्षर डेटा से जुड़ा हुआ है और फिर दोनों को सत्यापनकर्ता के पास भेजा जाता है।
- सत्यापनकर्ता डिजिटल (अंकीय) हस्ताक्षर और सत्यापन कुंजी को सत्यापन एल्गोरिथ्म (कलनविधि) में प्रविष्ट करता है। सत्यापन एल्गोरिथ्म (कलनविधि) आउटपुट (निर्गत) के रूप में कुछ मान देता है।
- सत्यापनकर्ता हैश (द्रुतान्वेषण) मान उत्पन्न करने के लिए प्राप्त डेटा पर समान हैश फंक्शन (द्रुतान्वेषण फलन) भी चलाता है।
- सत्यापन के लिए, सत्यापन एल्गोरिथ्म (कलनविधि) के इस हैश (द्रुतान्वेषण) मान और आउटपुट (निर्गत) की तुलना की जाती है। तुलना परिणाम के आधार पर, सत्यापनकर्ता यह तय करता है कि डिजिटल (अंकीय) हस्ताक्षर मान्य है या नहीं।

  डिजिटल (अंकीय) हस्ताक्षर योजना के प्रारूप को निम्नलिखित चित्र में दर्शाया गया है –



(चित्र क्र0 7.2)

चूंकि डिजिटल (अंकीय) हस्ताक्षर हस्ताक्षरकर्ता की व्यक्तिगत कुंजी द्वारा बनाया गया है और किसी और के पास यह कुंजी नहीं हो सकती है, अतः हस्ताक्षरकर्ता भविष्य में डेटा पर हस्ताक्षर करने से इनकार नहीं कर सकता।

यह ध्यान दिया जाना चाहिए कि एल्गोरिथ्म (कलनविधि) पर हस्ताक्षर करके सीधे डेटा पर हस्ताक्षर करने के स्थान पर, आमतौर पर डेटा का एक हैश बनाया जाता है। चूँकि डेटा का हैश (द्रुतान्वेषण) डेटा का एक अद्यतीय प्रतिनिधित्व है, इसलिए डेटा के स्थान पर हैश (द्रुतान्वेषण) पर हस्ताक्षर करना पर्याप्त है। हस्ताक्षर करने के लिए सीधे डेटा के स्थान पर हैश (द्रुतान्वेषण) का उपयोग करने का सबसे महत्वपूर्ण कारण योजना की दक्षता है।

मान लें कि RSA का उपयोग हस्ताक्षर एल्गोरिथ्म (कलनविधि) के रूप में किया जाता है। जैसा कि सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) में चर्चा की गई है, RSA का उपयोग करके एन्क्रिप्शन/हस्ताक्षर करने की प्रक्रिया में मॉड्यूलर घातांक सम्मिलित है।

मॉड्यूलर घातांक के माध्यम से बड़े डेटा पर हस्ताक्षर करना संगणन रूप से महंगा और समय लेने वाला है। डेटा का हैश (द्रुतान्वेषण) डेटा का एक अपेक्षाकृत छोटा डाइजेस्ट (पाचन) है, इसलिए पूरे डेटा पर हस्ताक्षर करने की तुलना में हैश (द्रुतान्वेषण) पर हस्ताक्षर करना अधिक उपयुक्त है।

7.3 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) का महत्वः

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) का उपयोग करने वाले डिजिटल (अंकीय) हस्ताक्षर को सूचना सुरक्षा प्राप्त करने के लिए बहुत महत्वपूर्ण और उपयोगी उपकरण माना जाता है।

संदेश के गैर–अस्वीकरण प्रदान करने की क्षमता के अतिरिक्त, डिजिटल (अंकीय) हस्ताक्षर संदेश प्रमाणीकरण और डेटा अखंडता भी प्रदान करता है। अब हम संक्षेप में यह देखेंगे कि यह डिजिटल (अंकीय) हस्ताक्षर द्वारा कैसे प्राप्त किया जाता है –

संदेश प्रमाणीकरणः जब सत्यापनकर्ता किसी प्रेषक की सार्वजनिक कुंजी का उपयोग करके डिजिटल (अंकीय) हस्ताक्षर को मान्य करता है, तो उसे विश्वास दिलाया जाता है कि हस्ताक्षर केवल प्रेषक द्वारा बनाए गए हैं जिनके पास संबंधित गुप्त व्यक्तिगत कुंजी है और कोई नहीं है।

डेटा इंटीग्रिटीः यदि किसी हमलावर के पास डेटा तक पहुँच है और इसे संशोधित करता है, तो प्राप्तकर्त्ता के अंत में डिजिटल (अंकीय) हस्ताक्षर सत्यापन विफल हो जाता है। संशोधित डेटा का हैश (द्रुतान्वेषण) और सत्यापन एल्गोरिथम (कलनविधि) द्वारा प्रदान किए गए आउटपुट (निर्गत) का मिलान नहीं होगा। इसलिए, रिसीवर यह मानते हुए संदेश को सुरक्षित रूप से अस्वीकार कर सकता है कि डेटा अखंडता का उल्लंघन हो गया है।

गैर–अस्वीकृतिः चूंकि यह माना जाता है कि केवल हस्ताक्षरकर्ता को हस्ताक्षर कुंजी का ज्ञान है, वह केवल किसी दिए गए डेटा पर अद्वितीय हस्ताक्षर बना सकता है। इस प्रकार प्राप्तकर्त्ता डेटा और डिजिटल (अंकीय) हस्ताक्षर को तीसरे पक्ष को साक्ष्य के रूप में प्रस्तुत कर सकता है यदि भविष्य में कोई विवाद उत्पन्न होता है।

डिजिटल (अंकीय) हस्ताक्षर योजना में सार्वजनिक–कुंजी एन्क्रिप्शन (कूट प्रक्रिया) को जोड़कर, हम एक क्रिप्टोसिस्टम (कूटप्रणाली) बना सकते हैं जो सुरक्षा के चार आवश्यक तत्व प्रदान कर सकते हैं – गोपनीयता, प्रमाणीकरण, अखंडता और गैर–प्रतिवाद।

7.4 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) के साथ एन्क्रिप्शन (कूट प्रक्रिया):

कई डिजिटल (अंकीय) संचारों में, गोपनीयता हासिल करने के लिए साधारण से एन्क्रिप्टेड (कूटित) संदेशों का आदान–प्रदान करना वांछनीय है। सार्वजनिक कुंजी एन्क्रिप्शन (कूट प्रक्रिया) योजना में, प्रेषक की एक सार्वजनिक (एन्क्रिप्शन) कुंजी खुले डोमेन में उपलब्ध है, और इसलिए कोई भी प्रेषक की पहचान को खराब कर सकता है और प्राप्तकर्त्ता को कोई भी एन्क्रिप्टेड (कूटित) संदेश भेज सकता है।

यह उपयोगकर्ताओं के लिए आवश्यक है कि वे PKC को एन्क्रिप्शन (कूट प्रक्रिया) के लिए डिजिटल (अंकीय) हस्ताक्षर के साथ–साथ एन्क्रिप्टेड डेटा (कूटित आँकड़ा) प्राप्त करने के लिए संदेश प्रमाणीकरण और गैर–अस्वीकृति का आश्वासन दें।

यह एन्क्रिप्शन (कूट प्रक्रिया) योजना के साथ डिजिटल (अंकीय) हस्ताक्षरों को जोड़कर संग्रहीत किया जा सकता है। अब हम संक्षेप में चर्चा करेंगे कि इस आवश्यकता को कैसे प्राप्त किया जाए। दो संभावनाएँ हैं, हस्ताक्षर के उपरान्त एनक्रिप्ट (कूटित) या एनक्रिप्ट (कूटित) के उपरान्त हस्ताक्षर।

हालाँकि, हस्ताक्षर के उपरान्त एनक्रिप्ट (कूटित) पर आधारित क्रिप्टो (कूट) प्रणाली का उपयोग रिसीवर द्वारा प्रेषक की पहचान को खराब करने के लिए किया जा सकता है और उस डेटा को तीसरे पक्ष को भेजा जा सकता है। इसलिए, यह विधि पसंद नहीं है। एनक्रिप्ट (कूटित) के उपरान्त हस्ताक्षर की प्रक्रिया अधिक विश्वसनीय और व्यापक रूप से अपनाई गई है। एन्क्रिप्टेड (कूटित) डेटा और उस पर हस्ताक्षर प्राप्त करने के बाद प्राप्तकर्त्ता, पहले प्रेषक की सार्वजनिक कुंजी का उपयोग करके हस्ताक्षर की पुष्टि करता है। हस्ताक्षर की वैधता सुनिश्चित करने के बाद, वह अपनी व्यक्तिगत कुंजी का उपयोग करके डिक्रिप्शन (अकूट प्रक्रिया) के माध्यम से डेटा को पुनः प्राप्त करता है।

किसी दस्तावेज को एन्क्रिप्ट करनाः

डिजिटल (अंकीय) हस्ताक्षर या एन्क्रिप्शन (कूट प्रक्रिया) का उपयोग करने के लिए हमारे पास एक डिजिटल (अंकीय) पहचान होना चाहिए जिसे डिजिटल (अंकीय) प्रमाणपत्र के रूप में भी जाना जाता है। एक डिजिटल पहचान/डिजिटल प्रमाणपत्र दो काम करता था। सबसे पहले, इसका उपयोग ईमेल या फाईल को एन्क्रिप्ट (कूटित) करने के लिए किया जा सकता है ताकि वे केवल उस व्यक्ति द्वारा पढ़े जा सकें जिनके लिए एन्क्रिप्ट (कूटित) किया गया है। दूसरा, इसका उपयोग हस्ताक्षर करने के लिए किया जा सकता है या यह सुनिश्चित करने के लिए कि यह मूल रूप से उसी अवस्था में आता है या नहीं और किसी ने चीजों को जोड़ा या बदला नहीं है, यह आश्वासन देने के लिए दस्तावेज पर एक डिजिटल (अंकीय) हस्ताक्षर रखता है।

एक सार्वजनिक और एक व्यक्तिगत कुंजी होती है। हमारी सार्वजनिक कुंजी सभी के साथ साझा की जाती है। अपनी व्यक्तिगत कुंजी को व्यक्तिगत रखा गया है। ये कुंजी पाठ दस्तावेज हैं जो यादृच्छिक संख्याओं और अक्षरों से प्रकट होते हैं, लेकिन उचित एल्गोरिथ्म (कलनविधि) के साथ, इन संख्याओं और अक्षरों में एक बहुत ही अद्वतीय गुण होता है।

यदि हम एक दस्तावेज को सार्वजनिक कुंजी के साथ एल्गोरिथ्म (कलनविधि) के माध्यम से चलाते हैं, तो हमें एक एन्क्रिप्टेड (कूटित) दस्तावेज या एक एन्क्रिप्टेड (कूटित) ईमेल वापस मिल जाता है।

सार्वजनिक कुंजी का उपयोग दस्तावेज को डिक्रिप्ट (अकूटित) करने के लिए नहीं किया जा सकता है। यह प्रक्रिया एक विधि है इसलिए यह महत्वपूर्ण नहीं है यदि अन्य लोगों के पास सार्वजनिक कुंजी है, तो वे दस्तावेज नहीं पढ़ सकते हैं।

दस्तावेज को डिक्रिप्ट (अकूटित) करने के लिए हमारे पास व्यक्तिगत कुंजी होनी चाहिए। यदि हम एन्क्रिप्टेड (कूटित) दस्तावेज को व्यक्तिगत कुंजी के साथ एल्गोरिथ्म (कलनविधि) में देते हैं, तो हमें मूल दस्तावेज वापस मिल जाएगा।

7.5 पब्लिक की इन्फ्रास्ट्रक्चर (सार्वजनिक कुंजी अवसंरचना):

सार्वजनिक कुंजी अवसंरचना (PKI) की सबसे विशिष्ट विशेषता यह है कि यह अंतर्निहित सुरक्षा सेवा को प्राप्त करने के लिए कुंजियों का एक युग्म का उपयोग करता है। कुंजी युग्म में व्यक्तिगत कुंजी और सार्वजनिक कुंजी शामिल हैं।

चूंकि सार्वजनिक कुंजी खुले डोमेन (प्रांत) में हैं, इसलिए उनका दुरुपयोग होने की संभावना है। इस प्रकार, इन कुंजियों को प्रबंधित करने के लिए किसी प्रकार के विश्वसनीय बुनियादी ढांचे को स्थापित करना और बनाए रखना आवश्यक है।

कुंजी प्रबंधनः

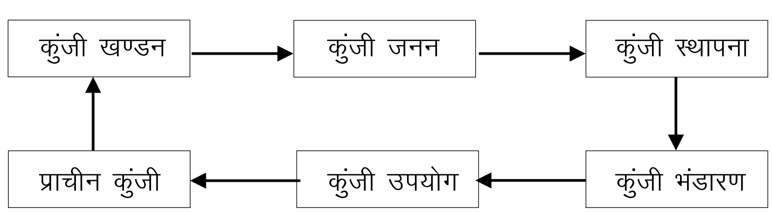
किसी भी क्रिप्टोसिस्टम (कूटप्रणाली) की सुरक्षा इस बात पर निर्भर करती है कि इसकी कुंजी कितनी सुरक्षित रूप से प्रबंधित की जाती है। क्रिप्टोग्राफिक (कूटलेखीय) कुंजियों की हैंडलिंग के लिए सुरक्षित प्रक्रियाओं के बिना, मजबूत क्रिप्टोग्राफिक (कूटलेखीय) योजनाओं के उपयोग के लाभ संभावित रूप से खो जाते हैं।

यह देखा गया है कि क्रिप्टोग्राफिक (कूटलेखीय) योजनाओं को उनके डिजाइन में कमियों के माध्यम से शायद ही कभी समझौता किया जाता है। हालांकि, वे अक्सर खराब कुंजी प्रबंधन के माध्यम से समझौता कर रहे हैं।

कुंजी प्रबंधन के कुछ महत्वपूर्ण पहलू हैं जो निम्न प्रकार हैं:

क्रिप्टोग्राफिक (कूटलेखीय) कुंजी डेटा के विशेष भागों के अलावा कुछ भी नहीं है। कुंजी प्रबंधन, क्रिप्टोग्राफिक (कूटलेखीय) कुंजियों के सुरक्षित प्रशासन को संदर्भित करता है।

निम्नांकित चित्र में दर्शाए अनुसार कुंजी प्रबंधन कुंजी के पूर जीवनचक्र से संबंधित हैः



(चित्र क्र0 7.3)

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) के लिए कुंजी प्रबंधन की दो विशिष्ट आवश्यकताएं हैं:

व्यक्तिगत कुंजी की गोपनीयताः कुंजी जीवनचक्र के दौरान, गुप्त कुंजियाँ सभी पक्षों से गुप्त रहनी चाहिए, सिवाय उनके जो स्वामी हैं और उनका उपयोग करने के लिए अधिकृत हैं।

सार्वजनिक कुंजी का आश्वासनः सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) में, सार्वजनिक कुंजी खुले डोमेन में होती है और इसे डेटा के सार्वजनिक भागों के रूप में देखा जाता है। डिफॉल्ट रूप से इस बात का कोई आश्वासन नहीं है कि क्या सार्वजनिक कुंजी सही है, जिसके साथ इसे संबद्ध किया जा सकता है, या इसका क्या उपयोग किया जा सकता है। इस प्रकार सार्वजनिक कुंजी के उद्देश्य के आश्वासन पर सार्वजनिक कुंजी के प्रमुख प्रबंधन को अधिक स्पष्ट रूप से ध्यान केंद्रित करने की आवश्यकता है।

सार्वजनिक कुंजी के 'आश्वासन की सबसे महत्वपूर्ण आवश्यकता' PKI के माध्यम से प्राप्त की जा सकती है, जो सार्वजनिक–कुंजी क्रिप्टोग्राफी (कूटलेखन) का समर्थन करने के लिए एक कुंजी प्रबंधन प्रणाली है।

PKI सार्वजनिक कुंजी का आश्वासन देता है। यह सार्वजनिक कुंजी और उनके वितरण की पहचान प्रदान करता है। PKI की संरचना में निम्नलिखित घटक शामिल हैं:

- सार्वजनिक कुंजी प्रमाणपत्र, जिसे आमतौर पर डिजिटल (अंकीय) प्रमाणपत्र कहा जाता है।
- व्यक्तिगत कुंजी टोकन।
- प्रमाणन प्राधिकरण।
- पंजीकरण प्राधिकरण।
- प्रमाणपत्र प्रबंधन प्रणाली।

PKI डिजिटल (अंकीय) प्रमाणपत्रों को बनाने, प्रबंधित करने, वितरित करने, उपयोग करने, संग्रहीत करने और बदलने और सार्वजनिक–कुंजी एन्क्रिप्शन (कूटप्रणाली) का प्रबंधन करने के लिए आवश्यक भूमिकाओं, नीतियों और प्रक्रियाओं का एक समूह है। PKI का उद्देश्य ई–कॉमर्स, इंटरनेट बैंकिंग और गोपनीय ईमेल जैसी नेटवर्क गतिविधियों की एक विस्तृत जानकारी के लिए सुरक्षित इलेक्ट्रॉनिक हस्तांतरण की सुविधा प्रदान करना है।

यह उन गतिविधियों के लिए आवश्यक है जहाँ सरल पासवर्ड एक अपर्याप्त प्रमाणीकरण पद्धति है और संचार में शामिल पक्षों की पहचान की पुष्टि करने और स्थानांतरित होने वाली जानकारी को मान्य करने के लिए अधिक कठोर प्रमाण की आवश्यकता होती है।

क्रिप्टोग्राफी (कूटलेखन) में, PKI एक ऐसी व्यवस्था है जो सार्वजनिक कुंजी को एन्टिटी की पहचान (जैसे लोगों और संगठनों) से बांधती है। बाइंडिंग एक प्रमाणपत्र प्राधिकारी (CA) द्वारा पंजीकरण और प्रमाण पत्र जारी करने की प्रक्रिया के माध्यम से स्थापित की जाती है। बाध्यकारी के आश्वासन स्तर के आधार पर, यह एक स्वचालित प्रक्रिया या मानव पर्यवेक्षण के तहत किया जा सकता है। PKI की भूमिका जो वैध और सही पंजीकरण का आश्वासन देती है उसे पंजीकरण प्राधिकरण (RA) कहा जाता है। RA डिजिटल प्रमाणपत्रों के अनुरोधों को स्वीकार करने और अनुरोध करने वाली इकाई को प्रमाणित करने के लिए जिम्मेदार है। माइक्रोसॉफ्ट PKI में, एक पंजीकरण प्राधिकरण को आमतौर पर एक अधीनस्थ CA कहा जाता है।

उस इकाई के बारे में जानकारी के आधार पर प्रत्येक CA डोमेन में एक इकाई विशिष्ट रूप से पहचानी जानी चाहिए। एक तृतीय–पक्ष सत्यापन प्राधिकरण (VA) CA की ओर से इस इकाई की जानकारी प्रदान कर सकता है।

PKI में विभिन्न प्रकार के प्रणाली हैं:

1. व्यक्तिगत और सार्वजनिक कुंजी प्रणालीः व्यक्तिगत कुंजी सिस्टम सममित क्रिप्टोग्राफी (कूटलेखन) हैं और एक सार्वजनिक सिस्टम असममित क्रिप्टोग्राफी (कूटलेखन) हैं। वर्तमान में, सार्वजनिक कुंजी प्रणाली सबसे आम हैं।

2. सममित एन्क्रिप्शन (कूट प्रक्रिया) प्रणालीः एक ही कुंजी का उपयोग एन्क्रिप्शन (कूट प्रक्रिया) और डिक्रिप्शन (अकूट प्रक्रिया) दोनों प्रक्रियाओं के लिए किया जाता है।

3. असममित एन्क्रिप्शन (कूट प्रक्रिया) प्रणालीः प्रत्येक प्रक्रिया के लिए एक पृथक कुंजी का उपयोग किया जाता है। एक कुंजी सार्वजनिक कुंजी है और दूसरी कुंजी व्यक्तिगत कुंजी है। यदि सार्वजनिक कुंजी के साथ कुछ एन्क्रिप्ट (कूटित) किया गया है, तो डिक्रिप्शन (अकूट प्रक्रिया) केवल व्यक्तिगत कुंजी के साथ किया जा सकता है। वैकल्पिक रूप से, यदि कुछ व्यक्तिगत कुंजी के साथ एन्क्रिप्ट (कूटित) किया गया है, तो डिक्रिप्शन (अकूट प्रक्रिया) केवल सार्वजनिक कुंजी के साथ किया जाना चाहिए।

CA कुंजी प्रदान करने वाली इकाई है। व्यक्तिगत कुंजी को अनुरोध करने वाले व्यक्ति को दिया जाता है। सार्वजनिक कुंजी को उपयोगकर्ताओं के लिए निर्देशिका में सार्वजनिक किया जाता है। कोई भी कभी भी यह पता नहीं कर सकता है कि किसी की व्यक्तिगत कुंजी क्या है, कभी भी इंटरनेट पर उपलब्ध नहीं है। व्यक्तिगत कुंजी का उपयोग उपयोगकर्ता पहचान को साबित करने और डिजिटल (अंकीय) प्रमाणपत्र को एन्क्रिप्ट (कूटित) करने के लिए किया जाता है। डिजिटल (अंकीय) कुंजी को सार्वजनिक कुंजी द्वारा डिक्रिप्ट (अकूटित) किया जाएगा, जो संदेश प्राप्तकर्त्ता द्वारा उपयोग किया जाता है।

PKI को सक्षम करने वाली कई कंपनियां हैं। डिजिटल (अंकीय) प्रमाणपत्र के लिए पंजीकरण प्रक्रिया RA के साथ शुरू होती है। CA को पता है कि उपयोगकर्ता को एक प्रमाण पत्र जारी किया जाएगा या नहीं। PKI में कई भाग सम्मिलित हैं। उचित रूप से सक्षम, ये सहज, पारदर्शी और सुरक्षित संचार प्रदान करते हैं।

7.6 डिजिटल सर्टिफिकेट (अंकीय प्रमाण पत्र):

सादृश्य के लिए, एक प्रमाण–पत्र को व्यक्ति को जारी किया गया आईडी कार्ड माना जा सकता है। लोग अपनी पहचान साबित करने के लिए ड्राइविंग लाइसेंस, पासपोर्ट जैसे आईडी कार्ड का इस्तेमाल करते हैं। एक डिजिटल (अंकीय) प्रमाण–पत्र या डिजिटल (अंकीय) सर्टिफिकेट इलेक्ट्रॉनिक दुनिया में एक ही मूल काम करता है, लेकिन एक अंतर के साथ।

डिजिटल (अंकीय) प्रमाण–पत्र न केवल लोगों को जारी किए जाते हैं बल्कि उन्हें कम्प्यूटर, सॉफ्टवेयर पैकेज या किसी और चीज से जारी किया जा सकता है, जिसे इलेक्ट्रॉनिक दुनिया में पहचान साबित करने की जरूरत है।

डिजिटल (अंकीय) प्रमाणपत्र ITU मानक X.509 पर आधारित हैं जो सार्वजनिक कुंजी प्रमाण–पत्र और प्रमाणन सत्यापन के लिए एक मानक प्रमाणपत्र प्रारूप को परिभाषित करता है। इसलिए डिजिटल प्रमाण–पत्रों को कभी–कभी X.509 प्रमाणपत्र भी कहा जाता है।

उपयोगकर्ता कुंजी से संबंधित सार्वजनिक कुंजी को CA द्वारा डिजिटल (अंकीय) प्रमाण–पत्रों में संग्रहीत किया जाता है, साथ ही साथ अन्य प्रासंगिक जानकारी जैसे क्लाइंट जानकारी, समाप्ति तिथि, उपयोग, जारीकर्ता आदि। CA पूरी तरह से इस पूरी जानकारी पर हस्ताक्षर करता है और प्रमाण–पत्र में डिजिटल (अंकीय) हस्ताक्षर शामिल करता है।

जिस किसी को भी सार्वजनिक कुंजी और क्लाइंट की संबंधित जानकारी के बारे में आश्वासन की आवश्यकता होती है, वह CA की सार्वजनिक कुंजी का उपयोग करके हस्ताक्षर सत्यापन प्रक्रिया करता है। सफल सत्यापन यह आश्वासन देता है कि प्रमाण–पत्र में दी गई सार्वजनिक कुंजी उस व्यक्ति की है जिसका विवरण प्रमाण–पत्र में दिया गया है।

CA अपनी सार्वजनिक कुंजी को प्रमाणित करने के लिए क्लाइंट से आवेदन स्वीकार करता है। क्लाइंट की पहचान की विधिवत पुष्टि करने के बाद, CA उस क्लाइंट को एक डिजिटल (अंकीय) प्रमाण–पत्र जारी करता है।

डिजिटल (अंकीय) प्रमाण–पत्र एक विश्वसनीय तृतीय पक्ष द्वारा जारी किया जाता है जो प्रेषक को प्राप्तकर्ता की पहचान और प्राप्तकर्ता को प्रेषक की पहचान को प्रमाणित करता है।

प्रमाण–पत्र धारक की पहचान को सत्यापित करने के लिए एक सर्टिफिकेट अथॉरिटी CA द्वारा जारी किया गया एक सर्टिफिकेट होता है। CA एक एन्क्रिप्टेड (कूटित) डिजिटल (अंकीय) प्रमाणपत्र जारी करता है जिसमें आवेदक की सार्वजनिक कुंजी और कई अन्य पहचान की जानकारी होती है। डिजिटल (अंकीय) हस्ताक्षर का उपयोग किसी विशेष व्यक्ति या संस्था के साथ सार्वजनिक कुंजी को जोड़ने के लिए किया जाता है।

डिजिटल (अंकीय) प्रमाण पत्र में शामिल हैं:

1. प्रमाण पत्र धारक का नाम।
2. सरल क्रमांक जो किसी प्रमाण–पत्र की विशिष्ट पहचान करने के लिए प्रयोग किया जाता है, व्यक्ति या प्रमाण पत्र द्वारा पहचानी गई इकाई।
3. समाप्ति की तारीख।

4. प्रमाण पत्र धारक की सार्वजनिक कुंजी की प्रतिलिपि। (संदेश और डिजिटल हस्ताक्षर एन्क्रिप्ट करने के लिए उपयोग किया जाता है)
5. प्रमाण पत्र जारी करने वाले प्राधिकारी का डिजिटल हस्ताक्षर।

डिजिटल हस्ताक्षर और संदेश के साथ डिजिटल (अंकीय) सर्टिफिकेट भी भेजा जाता है।

डिजिटल (अंकीय) प्रमाण–पत्र बनाम डिजिटल हस्ताक्षरः

डिजिटल (अंकीय) हस्ताक्षर का उपयोग प्रामाणिकता, अखंडता, गैर–प्रतिशोध, अर्थात् को सत्यापित करने के लिए किया जाता है। यह आश्वासन देता है कि संदेश ज्ञात उपयोगकर्ता द्वारा भेजा गया है और संशोधित नहीं है, जबकि डिजिटल (अंकीय) प्रमाण–पत्र का उपयोग उपयोगकर्ता की पहचान, शायद प्रेषक या प्राप्तकर्त्ता को सत्यापित करने के लिए किया जाता है। इस प्रकार, डिजिटल (अंकीय) हस्ताक्षर और प्रमाण–पत्र भिन्न ऑब्जेक्ट हैं लेकिन दोनों का उपयोग सुरक्षा के लिए किया जाता है। अधिकांश वेबसाइट अपने उपयोगकर्ताओं का विश्वास बढ़ाने के लिए डिजिटल (अंकीय) प्रमाण–पत्र का उपयोग करती हैं।

डिजिटल (अंकीय) प्रमाणपत्र प्राप्त करने की प्रक्रियाः

निम्नलिखित चरण डिजिटल (अंकीय) प्रमाणपत्र प्राप्त करने की प्रक्रिया को दर्शाता है।

1. कुंजी युग्म जनित करें: उपयोगकर्ता A सार्वजनिक और व्यक्तिगत कुंजी युग्म बनाता है या उनके संगठन में कुछ प्राधिकरण द्वारा एक कुंजी युग्म को सौंपा जाता है।
2. CA प्रमाणपत्र अनुरोधः उपयोगकर्ता A पहले CA सर्वर के प्रमाण पत्र का अनुरोध करता है।
3. CA सर्टिफिकेट जारी करनाः CA अपने सर्टिफिकेट के साथ उत्तर देता है। इसमें इसके व्यक्तिगत कुंजी का उपयोग करके सार्वजनिक कुंजी और इसके हस्ताक्षरित डिजिटल (अंकीय) हस्ताक्षर सम्मिलित हैं।
4. जानकारी एकत्र करनाः उपयोगकर्ता A अपने प्रमाण पत्र को प्राप्त करने के लिए CA सर्वर द्वारा आवश्यक सभी जानकारी एकत्र करता है। इस जानकारी में उपयोगकर्ता CA ईमेल पता, उंगलियों के निशान आदि शामिल हो सकते हैं कि CA को निश्चित होना चाहिए कि उपयोगकर्ता CA का आश्वासन है कि वह कौन है।
5. प्रमाणपत्र अनुरोध भेजें: उपयोगकर्ता A अपनी सार्वजनिक कुंजी और अतिरिक्त जानकारी के साथ CA को एक प्रमाणपत्र अनुरोध भेजता है। प्रमाणपत्र अनुरोध CA के सार्वजनिक कुंजी द्वारा हस्ताक्षरित होते हैं।
6. CA उपयोगकर्ता A की पुष्टि करता है: CA को प्रमाणपत्र अनुरोध मिलता है, उपयोगकर्ता A की पहचान की पुष्टि करता है और उपयोगकर्ता A के लिए एक प्रमाण पत्र बनाता है, जिससे उसकी पहचान और उसकी सार्वजनिक कुंजी बंध जाती है। CA का हस्ताक्षर प्रमाणपत्र की प्रामाणिकता की पुष्टि करता है।
7. CA द्वारा प्रमाणपत्र जारी करनाः सीए उपयोगकर्ता CA को प्रमाण पत्र जारी करता है।

उदाहरण के लिए, उपयोगकर्ता A सुरक्षित रूप से उपयोगकर्ता B के साथ संवाद करना चाहता है। और उपयोगकर्ता B को सुरक्षित संचार के लिए एक डिजिटल (अंकीय) प्रमाणपत्र की आवश्यकता है। सबसे पहले, उपयोगकर्ता B को CA से एक डिजिटल (अंकीय) प्रमाणपत्र प्राप्त करना होगा। प्रमाणपत्र प्राप्त करने के लिए उपयोगकर्ता B निम्न प्रक्रिया का उपयोग करता है–

1. डिजिटल (अंकीय) प्रमाणपत्र प्राप्त करने के लिए, पहली बार, उपयोगकर्ता B, RA को एक अनुरोध भेजता है। RA अनुरोधकर्ता की पहचान की पुष्टि करने के लिए जिम्मेदार है। यह कोई प्रमाण पत्र जारी नहीं करता है। RA को अपनी पहचान साबित करने के लिए B अपने ड्राइविंग लाइसेंस, व्यावसायिक दस्तावेज या किसी अन्य पहचान जानकारी का उपयोग कर सकता है। एक बार जब RA, B की पहचान जानकारी से संतुष्ट हो जाता है, तो वह डिजिटल (अंकीय) प्रमाणपत्र जारी करने के लिए, उपयोगकर्ता B की ओर से CA को अनुरोध भेजता है।
2. CA, B की सार्वजनिक कुंजी और अन्य पहचान जानकारी का उपयोग करके डिजिटल (अंकीय) प्रमाण पत्र बनाता है। इस प्रमाणपत्र को बनाने के लिए उपयोग किया जाने वाला मानक X-509 है। सार्वजनिक/व्यक्तिगत कुंजी जोड़ी CA या उपयोगकर्ता B द्वारा बनाई जा सकती है।

जब CA ने उपयोगकर्ता की ओर से सार्वजनिक कुंजी बनाई है, तो उसे B को सार्वजनिक और व्यक्तिगत कुंजी बनाने के लिए व्यक्तिगत कुंजी को सुरक्षित रूप से B में भेजने की आवश्यकता है। कुंजी युग्म, डिजिटल (अंकीय) प्रमाणपत्र बनाने के लिए इसे सार्वजनिक रूप से CA को सुरक्षित रूप से कुंजी भेजने की आवश्यकता है।

3. डिजिटल (अंकीय) प्रमाण पत्र की प्रामाणिकता, अखंडता और गैर–प्रतिक्षेप सुनिश्चित करने के लिए CA अपनी स्वयं की व्यक्तिगत कुंजी के साथ प्रमाण पत्र पर हस्ताक्षर करता है। अंत में, CA, B को प्रमाणपत्र वापस भेजता है, जिसका उपयोग सुरक्षित संचार स्थापित करने के लिए किया जा सकता है।

उपर्युक्त चरण यह सुनिश्चित करते हैं कि उपयोगकर्ता B के पास एक डिजिटल (अंकीय) प्रमाण पत्र है जिसका उपयोग कोई अन्य उपयोगकर्ता B के साथ संचार शुरू करने के लिए कर सकता है। B के डिजिटल (अंकीय) प्रमाणपत्र पर संचार शुरू करने के लिए, A निम्नलिखित चरणों का उपयोग करता है:

1. B के डिजिटल (अंकीय) प्रमाणपत्र के लिए एक प्रमाणपत्र भंडार के लिए एक अनुरोध भेजता है, जिसे सार्वजनिक निर्देशिका के रूप में भी जाना जाता है, जो CA का एक भाग है।

2. जब A को B का प्रमाणपत्र प्राप्त होता है, तो वह CA के सार्वजनिक कुंजी का उपयोग करके CA के डिजिटल (अंकीय) हस्ताक्षर का परीक्षण करके वेब ब्राउजर की सहायता से इसे सत्यापित करता है। फिर A संदेश को एन्क्रिप्ट (कूटित) करने के लिए प्रमाणपत्र द्वारा आपूर्ति की गई B की सार्वजनिक कुंजी का उपयोग करता है।

3. जब B एन्क्रिप्टेड (कूटित) संदेश प्राप्त करता है, तो B संदेश को डिक्रिप्ट (अकूटित) करने के लिए अपनी व्यक्तिगत कुंजी का उपयोग करता है। स्मरण रहे कि A को छोड़कर कोई भी इस संदेश को डिक्रिप्ट (अकूटित) नहीं कर पाएगा क्योंकि A की व्यक्तिगत कुंजी किसी के साथ साझा नहीं की गई है।

कुछ प्रसिद्ध प्रमाणपत्र अधिकारी निम्न हैं:

- VeriSign
- Thawte
- Comodo Limited
- DigiCert
- Network Solutions, LLC

7.7 प्रमाणन प्राधिकरण (CA):

जैसा कि ऊपर चर्चा की गई है, CA क्लाइंट को प्रमाणपत्र जारी करता है और प्रमाणपत्र को सत्यापित करने के लिए अन्य उपयोगकर्ताओं की सहायता करता है। CA प्रमाणपत्र जारी करने के लिए पूछ रहे क्लाइंट की पहचान को सही ढंग से पहचानने की जिम्मेदारी लेता है, और यह सुनिश्चित करता है कि प्रमाणपत्र के अंदर स्थित जानकारी सही है और डिजिटल (अंकीय) रूप से इस पर हस्ताक्षर करता है।

CA के प्रमुख कार्यः

CA के प्रमुख कार्य निम्न हैं:

कुंजी युग्म जनित करनाः CA स्वतंत्र रूप से या क्लाइंट के साथ संयुक्त रूप से एक कुंजी युग्म जनित कर सकता है।

डिजिटल (अंकीय) प्रमाणपत्र जारी करनाः सीए को पासपोर्ट एजेंसी के PKI के बराबर माना जा सकता है। क्लाइंट द्वारा अपनी पहचान की पुष्टि करने के उपरांत CA एक प्रमाण पत्र जारी करता है। CA तब प्रमाणपत्र में निहित विवरणों के संशोधन को रोकने के लिए प्रमाण पत्र पर हस्ताक्षर करता है।

प्रमाणपत्र का प्रकाशनः CA को प्रमाण पत्र प्रकाशित करने की आवश्यकता है ताकि उपयोगकर्ता उन्हें खोज सकें। इसे प्राप्त करने की दो विधियाँ हैं। एक इलेक्ट्रॉनिक टेलीफोन निर्देशिका के बराबर में प्रमाण पत्र प्रकाशित करना है। दूसरा यह है कि हम अपने प्रमाणपत्र को उन लोगों को भेजें जिन्हें हमें लगता है कि एक या दूसरे माध्यम से इसकी आवश्यकता हो सकती है।

प्रमाणपत्र का प्रमाणनः CA क्लाइंट के डिजिटल (अंकीय) प्रमाणपत्र पर अपने हस्ताक्षर के सत्यापन में सहायता के लिए अपनी सार्वजनिक कुंजी को उपलब्ध कराता है।

प्रमाणपत्रों का निरसनः कई बार, CA किसी कारण से जारी किए गए प्रमाणपत्र को रद्द कर देता है जैसे उपयोगकर्ता द्वारा निजी कुंजी से समझौता करना या ग्राहक पर विश्वास खोना। निरसन के बाद, CA सभी निरस्त प्रमाण पत्र की सूची रखता है।

प्रमाण पत्र की श्रेणियाँः

प्रमाणपत्र के चार विशिष्ट वर्ग हैंः

श्रेणी 1 – ईमेल पते की आपूर्ति करके इन प्रमाणपत्रों को आसानी से प्राप्त किया जा सकता है।

श्रेणी 2 – इन प्रमाण पत्रों के लिए अतिरिक्त व्यक्तिगत जानकारी की आवश्यकता होती है।

श्रेणी 3 – ये प्रमाण पत्र केवल अनुरोधकर्ता की पहचान के बारे में परीक्षण के उपरांत क्रय किये जा सकते हैं।

श्रेणी 4 – वे सरकारों और वित्तीय संगठनों द्वारा उपयोग किए जा सकते हैं जिनके लिए बहुत उच्च स्तर के विश्वास की आवश्यकता होती है।

पंजीकरण प्राधिकरण (Registration Authority - RA):

CA अपनी पहचान की पुष्टि करने के लिए प्रमाणपत्र का अनुरोध करने वाले व्यक्ति या कंपनी पर आवश्यक परीक्षण करने के लिए एक तृतीय–पक्ष पंजीकरण प्राधिकरण का उपयोग कर सकता है। RA क्लाइंट को CA के रूप में दिखाई दे सकता है, लेकिन वे वास्तव में जारी किए गए प्रमाण पत्र पर हस्ताक्षर नहीं करते हैं।

प्रमाणपत्र प्रबंधन प्रणालीः

प्रबंधन प्रणाली वह है जिसके माध्यम से प्रमाण पत्र प्रकाशित, अस्थायी या स्थायी रूप से निलंबित, नवीनीकृत या निरस्त किए जाते हैं।

प्रमाणपत्र प्रबंधन प्रणाली आम तौर पर प्रमाणपत्र को डिलीट नहीं करते हैं, क्योंकि हो सकता है कि किसी समय कानूनी कारणों से अपनी स्थिति को साबित करना आवश्यक हो। CA संबद्ध RA प्रमाणपत्र प्रबंधन प्रणाली के साथ अपने उत्तरदायित्वों को ट्रैक करने में सक्षम होता है।

मूल्यवान होने के लिए सार्वजनिक–कुंजी क्रिप्टोग्राफी (कूटलेखन) के लिए, उपयोगकर्ताओं को यह आश्वासन दिया जाना चाहिए कि दूसरे पक्ष जिनके साथ वे संवाद करते हैं, वे सुरक्षित हैं, उनकी पहचान और कुंजी वैध और विश्वसनीय हैं। इस आश्वासन को प्रदान करने के लिए, PKI के सभी उपयोगकर्ताओं की एक पंजीकृत पहचान होनी चाहिए। इन पहचानों को एक डिजिटल (अंकीय) प्रारूप में संग्रहीत किया जाता है जिसे सार्वजनिक कुंजी प्रमाणपत्र के रूप में जाना जाता है। प्रमाणन प्राधिकारी डिजिटल (अंकीय) प्रमाणपत्र बनाने के लिए लोगों, प्रक्रियाओं और उपकरणों का प्रतिनिधित्व करते हैं जो उपयोगकर्ताओं के नामों को उनकी सार्वजनिक कुंजी में सुरक्षित रूप से बाँधते हैं। प्रमाण पत्र बनाने में, CA एक PKI में विश्वास के एजेंट के रूप में कार्य करते हैं। जब तक उपयोगकर्ता प्रमाणपत्र जारी करने और प्रबंधित करने के लिए CA और उसकी व्यावसायिक नीतियों पर भरोसा करते हैं, तब तक वे CA द्वारा जारी किए गए प्रमाणपत्रों पर भरोसा कर सकते हैं। इसे थर्ड–पार्टी ट्रस्ट के रूप में जाना जाता है। CA डेटा के एक सेट पर डिजिटल (अंकीय) रूप से हस्ताक्षर करके उपयोगकर्ताओं के लिए प्रमाण पत्र बनाते हैं जिसमें निम्न जानकारी सम्मिलित होती हैः

- एक विशिष्ट नाम के प्रारूप में उपयोगकर्ता का नाम। विशिष्ट नाम उपयोगकर्ता के नाम को निर्दिष्ट करता है और उपयोगकर्ता को विशिष्ट रूप से पहचानने के लिए आवश्यक किसी भी अतिरिक्त विशेषताओं (उदाहरण के लिए, विशिष्ट नाम में उपयोगकर्ता का कर्मचारी संख्या सम्मिलित हो सकता है)।
- उपयोगकर्ता की एक सार्वजनिक कुंजी। सार्वजनिक कुंजी की आवश्यकता है ताकि अन्य उपयोगकर्ता के लिए एन्क्रिप्ट (कूटित) कर सकें या उपयोगकर्ता के डिजिटल (अंकीय) हस्ताक्षर को सत्यापित कर सकें।
- प्रमाणपत्र की वैधता अवधि (या जीवनकाल) (एक आरंभ तिथि और अंतिम तिथि)।
- विशिष्ट संचालन जिसके लिए सार्वजनिक कुंजी का उपयोग किया जाना है (चाहे डेटा एन्क्रिप्ट करने के लिए, डिजिटल (अंकीय) हस्ताक्षर सत्यापित करने के लिए, या दोनों)।

किसी प्रमाणपत्र पर CA का हस्ताक्षर प्रमाणपत्र की सामग्री के साथ किसी भी छेड़छाड़ को आसानी से पता लगाने की अनुमति देता है। (प्रमाण पत्र पर CA का हस्ताक्षर छेड़छाड़ का पता लगाने वाली एक मुहर के समान है। प्रमाण पत्र की सामग्री के साथ किसी भी छेड़छाड़ का आसानी से पता लगाया जाता है) जब तक किसी प्रमाणपत्र पर CA के हस्ताक्षर को सत्यापित किया जा सकता है, तब तक प्रमाणपत्र में अखंडता होती है। चूंकि CA के हस्ताक्षर को सत्यापित करके एक प्रमाण पत्र की अखंडता निर्धारित की जा सकती है, इसलिए प्रमाण पत्र स्वाभाविक रूप से सुरक्षित हैं और इसे पूरी तरह से सार्वजनिक तरीके से वितरित किया जा सकता है (उदाहरण के लिए, सार्वजनिक रूप से सुलभ निर्देशिका प्रणालियों के माध्यम से)।

किसी प्रमाणपत्र से सार्वजनिक कुंजी प्राप्त करने वाले उपयोगकर्ताओं को आश्वासन दिया जा सकता है कि सार्वजनिक कुंजी मान्य है। उपयोगकर्ता यह भरोसा कर सकते हैं कि प्रमाणपत्र और उससे जुड़ी सार्वजनिक कुंजी प्रतिष्ठित नाम से निर्दिष्ट इकाई से संबंधित है। उपयोगकर्ताओं को यह भी भरोसा है कि सार्वजनिक कुंजी अभी भी इसकी परिभाषित वैधता अवधि के भीतर है। इसके अतिरिक्त, उपयोगकर्ताओं को आश्वासन दिया जाता है कि सार्वजनिक कुंजी का उपयोग उस तरीके से सुरक्षित रूप से किया जा सकता है जिसके लिए वह CA द्वारा प्रमाणित किया गया था।

7.8 CA का वंशानुक्रम:

विशाल नेटवर्क और वैश्विक संचार की आवश्यकताओं के साथ, यह व्यावहारिक रूप से संभव नहीं है कि केवल एक विश्वसनीय CA हो, जिनसे सभी उपयोगकर्ता अपने प्रमाण पत्र प्राप्त करते हैं। दूसरे, केवल एक CA की उपलब्धता से कठिनाइयों का सामना करना पड़ सकता है यदि CA से समझौता किया जाता हो।

इस दशा में, वंशानुक्रमित प्रमाणन मॉडल सामने आता है क्योंकि यह सार्वजनिक कुंजी प्रमाणपत्रों को उन वातावरणों में उपयोग करने की अनुमति देता है जहाँ दो संचार पक्षों का एक ही CA के साथ विश्वसनीय संबंध नहीं होता है।

मूल CA वंशानुक्रम के शीर्ष पर है और मूल CA का प्रमाण पत्र एक स्व–हस्ताक्षरित प्रमाण पत्र है। CAs, जो सीधे मूल CA के अधीनस्थ हैं (उदाहरण के लिए, CA 1 और CA 2) एक CA प्रमाण पत्र रखते हैं जो मूल CA द्वारा हस्ताक्षरित हैं।

वंशानुक्रम में अधीनस्थ CA के अंतर्गत रहने वाले CA (उदाहरण के लिए, CA 5 और CA 6) के पास उच्च स्तर के अधीनस्थ CA द्वारा हस्ताक्षरित अपने CA प्रमाण पत्र होते हैं। CA वंशानुक्रम प्रमाणपत्र श्रृंखला में परिलक्षित होते हैं। एक प्रमाणपत्र श्रृंखला वंशानुक्रम की एक शाखा से वंशानुक्रम के मूल तक प्रमाण–पत्र का मार्ग बताती है।

एक प्रमाण पत्र श्रृंखला का सत्यापन यह सुनिश्चित करने की प्रक्रिया है कि एक विशिष्ट प्रमाण पत्र श्रृंखला वैध, सही तरीके से हस्ताक्षरित और भरोसेमंद है। निम्नलिखित प्रक्रिया एक प्रमाण पत्र श्रृंखला की पुष्टि करती है, जो प्रमाणीकरण के लिए प्रस्तुत प्रमाण पत्र के साथ आरंभ होती है:

- एक क्लाइंट जिसकी सत्यता की पुष्टि की जा रही है, वह अपने प्रमाण पत्र की आपूर्ति करता है, आम तौर पर मूल CA तक प्रमाण पत्र की श्रृंखला के साथ।
- सत्यापनकर्ता प्रमाण पत्र लेता है और जारीकर्ता की सार्वजनिक कुंजी का उपयोग करके सत्यापन करता है। जारीकर्ता की सार्वजनिक कुंजी जारीकर्ता के प्रमाण पत्र में पाई जाती है जो क्लाइंट के प्रमाण पत्र के आगे की श्रृंखला में होती है।
- अब यदि उच्च CA जिसने जारीकर्ता के प्रमाण पत्र पर हस्ताक्षर किए हैं, तो सत्यापनकर्ता द्वारा भरोसा किया जाता है, सत्यापन सफल होता है और यहाँ रुक जाता है।
- जारीकर्ता के प्रमाण पत्र को उसी प्रकार सत्यापित किया जाता है जैसा कि उपरोक्त चरणों में क्लाइंट के लिए किया गया है। यह प्रक्रिया तब तक जारी रहती है जब तक कि भरोसेमंद CA मध्य में नहीं मिल जाता है या फिर यह मूल CA तक जारी रहता है।

7.9 डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) के अनुप्रयोग:

डिजिटल (अंकीय) हस्ताक्षर ई–मेल जैसे संदेश पर हस्ताक्षर करने के अतिरिक्त कई अनुप्रयोग प्रदान करते हैं। किसी भी प्रकार की फाइल के लिए एक डिजिटल (अंकीय) हस्ताक्षर बनाया जा सकता है। डिजिटल (अंकीय) हस्ताक्षर तब साक्ष्य के रूप में उपयोग किया जा सकता है कि डिजिटल (अंकीय) हस्ताक्षर बनाने के बाद फाइल को संशोधित नहीं किया गया था। इसका उपयोग फाइल को विशिष्ट बनाने के लिए भी किया जा सकता है, उदाहरण के लिए फाइल में एक सरल क्रमांक जोड़कर और परिणाम पर हस्ताक्षर करना।

वेब सर्वर्स का प्रमाणीकरणः

सार्वजनिक कुंजी क्रिप्टोग्राफी (कूटलेखन) का उपयोग करके एक वेब ब्राउजर और सर्वर एक दूसरे के साथ सुरक्षित रूप से संवाद कर सकते हैं। ब्राउजर सर्वर की सार्वजनिक कुंजी का उपयोग करके सत्र कुंजी को एन्क्रिप्ट (कूटित) कर सकता है और इसे सर्वर पर भेज सकता है।

इस अनुप्रयोग में वेब ब्राउजर आमतौर पर सर्वर से इस सार्वजनिक कुंजी वाले प्रमाणपत्र का अनुरोध करके सर्वर की सार्वजनिक कुंजी की एक प्रति प्राप्त करता है। इस प्रमाण पत्र पर कुछ विश्वसनीय तीसरे पक्ष द्वारा हस्ताक्षर किए गए हैं। इस विश्वसनीय तृतीय पक्ष की सार्वजनिक कुंजी पहले से वेब ब्राउजर में प्रोग्राम की गई है। इस सार्वजनिक कुंजी का उपयोग करके ब्राउजर यह निर्धारित कर सकता है कि प्रमाणपत्र प्रामाणिक है। ब्राउजर तब जानता है कि उसके पास सही सार्वजनिक कुंजी है।

टाइमस्टैम्पिंग सेवाएंः

संदेश के डिजिटल (कूटित) हस्ताक्षर को जिस अंतर्दृष्टि से देखा जा सकता है, वह संदेश से पूरी तरह से अलग हो सकता है, जिसने कई दिलचस्प नए अनुप्रयोगों को जन्म दिया है। अब उदाहरण के लिए डिजिटल (कूटित) टाइमस्टैम्पिंग सेवा की पेशकश करना संभव है। यह मूल रूप से एक अखबार में डिजिटल (कूटित) हस्ताक्षर प्रकाशित करने के उपरोक्त उदाहरण की तरह काम करता है।

हस्ताक्षरित कम्प्यूटर प्रोग्रामः

डिजिटल (अंकीय) हस्ताक्षर का उपयोग सॉफ्टवेयर अनुप्रयोगों को प्रमाणित करने के लिए भी किया जा सकता है। कम्प्यूटर प्रोग्राम का निर्माता निष्पादन योग्य के लिए एक डिजिटल (अंकीय) हस्ताक्षर उत्पन्न कर सकता है। जब कोई उपयोगकर्ता प्रोग्राम डाउनलोड करता है, तो वह सत्यापित कर सकता है कि डिजिटल (अंकीय) हस्ताक्षर सही है। तब वह जानता है कि यह प्रोग्राम वास्तव में उस विशेष निर्माता द्वारा बनाया गया था। यदि वह उस निर्माता पर भरोसा करता है, तो वह सुरक्षित रूप से एप्लिकेशन इंस्टॉल कर सकता है। बेशक निर्माता आश्वासन देता है कि एप्लिकेशन कुछ भी दुर्भावनापूर्ण नहीं करेगा।

डिजिटल (अंकीय) हस्ताक्षर प्रमाण पत्र व्यवसाय का ऑनलाइन संचालन करते समय व्यक्तिगत धारक की व्यक्तिगत जानकारी के विवरण को प्रमाणित करने में सहायक होते हैं।

कम लागत और समयः शारीरिक रूप से हार्ड कॉपी दस्तावेजों पर हस्ताक्षर करने और उन्हें ई–मेल के माध्यम से भेजने के लिए स्कैन करने के स्थान पर, आप डिजिटल (अंकीय) रूप से पीडीएफ फाइल्स पर हस्ताक्षर कर सकते हैं और उन्हें बहुत जल्दी भेज सकते हैं।

डिजिटल (अंकीय) हस्ताक्षर प्रमाण–पत्र धारक को किसी व्यवसाय का संचालन करने या अधिकृत करने के लिए भौतिक रूप से मौजूद नहीं होना पड़ता है।

डेटा अखंडताः दस्तावेज जो डिजिटल (अंकीय) रूप से हस्ताक्षरित हैं, उन्हें हस्ताक्षर करने के बाद परिवर्तित या संपादित नहीं किया जा सकता है, जो डेटा को सुरक्षित और सुरक्षित बनाता है।

सरकारी एजेंसियां अक्सर इन प्रमाणपत्रों को क्रॉस–चेक करने और व्यापार लेनदेन को सत्यापित करने के लिए कहती हैं।

दस्तावेजों की प्रामाणिकताः डिजिटली (अंकीय) हस्ताक्षरित दस्तावेज प्राप्तकर्त्ता को हस्ताक्षरकर्ता की प्रामाणिकता के प्रति आश्वस्त होने का विश्वास दिलाते हैं। जाली दस्तावेजों के बारे में चिंतित हुए बिना वे ऐसे दस्तावेजों के आधार पर कार्रवाई कर सकते हैं।

डिजिटल (अंकीय) हस्ताक्षर का उपयोग हस्तलिखित हस्ताक्षर के समान है। डिजिटल (अंकीय) हस्ताक्षर किसी व्यक्ति को प्रमाणित करने के लिए डिजिटल (अंकीय) कुंजी का उपयोग करता है। किसी भी दस्तावेज से जुड़ा एक डिजिटल (अंकीय) हस्ताक्षर प्रमाणपत्र भारत में आईटी कानून के अनुसार हस्ताक्षर धारक द्वारा बाध्यकारी प्रतिबद्धता है। डिजिटल हस्ताक्षर का उपयोग कठिन हो रहा है क्योंकि हस्तलिखित हस्ताक्षर के विपरीत, डिजिटल (अंकीय) हस्ताक्षर का नकली या नकली होना असंभव माना जाता है। तकनीकी प्रगति के साथ हम कलम और कागज की दुनिया से दूर इलेक्ट्रॉनिक युग में जा रहे हैं। अब एक दिन के अधिकांश सरकारी और निजी निविदाएं केवल इलेक्ट्रॉनिक रूप से एकत्र की जाती हैं। भारत में, आयकर, बिक्री कर आदि जैसे करों को इलेक्ट्रॉनिक रूप से दर्ज करना अधिकांश के लिए अनिवार्य है। इस सभी इलेक्ट्रॉनिक लेनदेन में डिजिटल (अंकीय) हस्ताक्षर का उपयोग कानूनी रूप से बाध्यकारी बनाने के लिए अनिवार्य है।

डिजिटल (अंकीय) हस्ताक्षर प्रमाणपत्र के उपयोग में सुरक्षित ईमेल भेजने के साथ–साथ वेब आधारित मौद्रिक लेनदेन भी शामिल हैं। हम अपने द्वारा विकसित किसी भी सॉफ्टवेयर के कोड हस्ताक्षर के लिए या अपने डोमेन नाम के स्वामित्व को साबित करने के लिए डिजिटल (अंकीय) सर्टिफिकेट का उपयोग कर सकते हैं। भारत में पेटेंट और ट्रेडमार्क पंजीकरण के लिए डिजिटल (अंकीय) हस्ताक्षर का उपयोग भी अनिवार्य है।

डिजिटल (अंकीय) हस्ताक्षर का उपयोग हालांकि इसके लिए प्रतिबंधित नहीं है। डिजिटल (अंकीय) हस्ताक्षर के उपयोग में बैंकिंग लेनदेन और मोबाइल सुरक्षा भी शामिल है।

अभ्यास

1. क्रिप्टोग्राफी डिजिटल सिग्नेचर (कूटलेखन अंकीय हस्ताक्षर) से क्या समझते हैं?
2. डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) का प्रारूप क्या होता है?
3. डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) के महत्व को समझाइए।
4. डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) के साथ एन्क्रिप्शन (कूट प्रक्रिया) को विस्तार से बताइए।
5. पब्लिक की इन्फ्रास्ट्रक्चर (सार्वजनिक कुंजी अवसंरचना) की अवधारणा को स्पष्ट कीजिए।
6. डिजिटल सर्टिफिकेट (अंकीय प्रमाण पत्र) से क्या समझते हैं?
7. प्रमाणन प्राधिकरण क्या होता है?
8. प्रमाणन प्राधिकरण के अनुक्रम को समझाइए।
9. डिजिटल सिग्नेचर (अंकीय हस्ताक्षर) के अनुप्रयोगों को लिखिए।

अध्याय – 8

नेटवर्क सुरक्षा – एक आकलन

आधुनिक युग में, संगठन कुशल और उत्पादक तरीके से संगठन में संपूर्ण जानकारी साझा करने के लिए कम्प्यूटर नेटवर्क पर विश्वास करते हैं। संगठनात्मक कम्प्यूटर नेटवर्क अब बड़े और सर्वव्यापी होते जा रहे हैं। यह मानते हुए कि प्रत्येक स्टाफ सदस्य के पास एक समर्पित कार्य केंद्र है, एक बड़े पैमाने पर कंपनी के पास कुछ हजारों वर्कस्टेशन और नेटवर्क पर कई सर्वर होंगे।

यह संभावना है कि ये कार्यस्थान केंद्र रूप से प्रबंधित नहीं किए जा सकते हैं, न ही इनकी परिधि सुरक्षा होगी। उपयोगकर्ताओं के मध्य साइबर जागरूकता के विभिन्न स्तर के साथ उनके पास कई प्रकार के ऑपरेटिंग सिस्टम, हार्डवेयर, सॉफ्टवेयर और प्रोटोकॉल (संदेशाचार) हो सकते हैं। अब कल्पना कीजिए, कंपनी नेटवर्क पर ये हजारों वर्कस्टेशन सीधे इंटरनेट से जुड़े हैं। इस प्रकार का असुरक्षित नेटवर्क एक हमले के लिए एक लक्ष्य बन जाता है जो मूल्यवान जानकारी रखता है और कमजोरियों को प्रदर्शित करता है।

8.1 भौतिक नेटवर्क:

एक नेटवर्क को दो या दो से अधिक कम्प्यूटिंग उपकरणों के रूप में परिभाषित किया गया है जो संसाधनों को कुशलतापूर्वक साझा करने के लिए एक साथ जुड़े हैं। इसके अतिरिक्त, दो या दो से अधिक नेटवर्क को एक साथ जोड़ने को इंटरनेटवर्किंग के रूप में जाना जाता है। इस प्रकार, इंटरनेट सिर्फ एक इंटरनेटवर्क है – परस्पर नेटवर्क का एक संग्रह।

अपने आंतरिक नेटवर्क की स्थापना के लिए, एक संगठन के पास विभिन्न विकल्प होते हैं। यह सभी कार्यस्थानों को जोड़ने के लिए एक वायर्ड (तार युक्त) नेटवर्क या वायरलेस (तार रहित) नेटवर्क का उपयोग कर सकता है। आजकल, ज्यादातर संगठन वायर्ड (तार युक्त) और वायरलेस (तार रहित) नेटवर्क दोनों के संयोजन का उपयोग कर रहे हैं।

वायर्ड और वायरलेस नेटवर्कः

एक वायर्ड नेटवर्क में, केबल के उपयोग से डिवाइस एक दूसरे से जुड़े होते हैं। आमतौर पर, वायर्ड नेटवर्क ईथरनेट प्रोटोकॉल पर आधारित होते हैं, जहाँ डिवाइस अलग–अलग स्विच में अनशीलड़ेड ट्विस्टेड पेयर (UTP) केबल का उपयोग करके जुड़े होते हैं। ये स्विच इंटरनेट तक पहुँचने के लिए नेटवर्क राउटर से जुड़े होते हैं।

वायरलेस नेटवर्क में, डिवाइस रेडियो प्रसारण के माध्यम से एक एक्सेस प्वाइंट से जुड़ा होता है। बाहरी नेटवर्क एक्सेस के लिए स्विच/राउटर हेतु एक्सेस पॉइंट्स को केबल के माध्यम से जोड़ा जाता है।

वायरलेस नेटवर्क ने उनके द्वारा पेश की गई गतिशीलता के कारण लोकप्रियता हासिल की है। मोबाइल उपकरणों को एक केबल से बांधने की आवश्यकता नहीं है और वायरलेस नेटवर्क रेंज के अंदर स्वतंत्र रूप से घूम सकते हैं। यह कुशल सूचना साझा करना सुनिश्चित करता है और उत्पादकता बढ़ाता है।

कमजोरियाँ और हमलेः

वायर्ड और वायरलेस नेटवर्क दोनों में उपलब्ध सामान्य भेद्यता एक नेटवर्क के लिए अनाधिकृत पहुँच है। एक हमलावर अपने डिवाइस को एक नेटवर्क से कनेक्ट कर सकता है हालांकि असुरक्षित हब/स्विच पोर्ट। इस संबंध में, वायरलेस नेटवर्क को वायर्ड नेटवर्क की तुलना में कम सुरक्षित माना जाता है, क्योंकि वायरलेस नेटवर्क को बिना किसी भौतिक कनेक्शन के आसानी से एक्सेस किया जा सकता है।

एक्सेस करने के बाद, एक हमलावर इस भेद्यता का फायदा उठा सकता है जैसे हमले शुरू करने के लिए।

- बहुमूल्य जानकारी चुराने के लिए पैकेट डेटा को सूँघना।
- एक नेटवर्क पर वैध उपयोगकर्ताओं के लिए सेवा की अस्वीकृति पैकेट के साथ नेटवर्क के माध्यम से।
- वैध मेजबान की भौतिक पहचान (MAC) को नष्ट करना और फिर डेटा चुराना या पुनः मैन–इन–द–मिडिल हमले शुरू करना।

8.2 नेटवर्क प्रोटोकॉल (संदेशाचार):

नेटवर्क प्रोटोकॉल नियमों का एक समूह है जो किसी नेटवर्क पर जुड़े उपकरणों के मध्य संचार को नियंत्रित करता है। उनमें कनेक्शन बनाने के लिए तकनीक सम्मिलित हैं, साथ ही भेजे गए और प्राप्त संदेशों के लिए डेटा पैकेजिंग के लिए नियमों को प्रारूपित करना भी सम्मिलित है।

कई कम्प्यूटर नेटवर्क प्रोटोकॉल प्रत्येक विशिष्ट उद्देश्यों के लिए डिजाइन किए गए हैं। लोकप्रिय और व्यापक रूप से उपयोग किए जाने वाले प्रोटोकॉल टीसीपी/आईपी से जुड़े उच्च और निचले स्तर के प्रोटोकॉल हैं।

8.2.1 TCP/IP प्रोटोकॉल (संदेशाचार):

ट्रांसमिशन कंट्रोल प्रोटोकॉल (Transmission Control Protocol - TCP) और इंटरनेट प्रोटोकॉल (Internet Protocol - IP) दो अलग–अलग कम्प्यूटर नेटवर्क प्रोटोकॉल हैं जिनका उपयोग ज्यादातर एक साथ किया जाता है। उनकी लोकप्रियता के कारण, वे नेटवर्क उपकरणों के सभी ऑपरेटिंग सिस्टम में निर्मित होते हैं।

OSI मॉडल में IP नेटवर्क लेयर (लेयर 3) से मेल खाती है जबकि TCP में ट्रांसपोर्ट लेयर (लेयर 4) से मेल खाता है। TCP/IP नेटवर्क संचार पर लागू होता है जहाँ पूरे IP नेटवर्क में डेटा पहुँचाने के लिए TCP परिवहन का उपयोग किया जाता है।

TCP/IP प्रोटोकॉल का उपयोग आमतौर पर अन्य प्रोटोकॉल जैसे कि HTTP, FTP, SSH के साथ एप्लिकेशन लेयर और ईथरनेट पर डेटा लिंक/फिजिकल लेयर में किया जाता है।

TCP/IP प्रोटोकॉल सूट 1980 में सुरक्षा पहलुओं के लिए बहुत कम चिंता के साथ एक इंटरनेटवर्किंग समाधान के रूप में बनाया गया था। इसे सीमित विश्वसनीय नेटवर्क में संचार के लिए विकसित किया गया था। हालाँकि, एक अवधि के दौरान, यह प्रोटोकॉल असुरक्षित इंटरनेट संचार के लिए वास्तविक मानक बन गया।

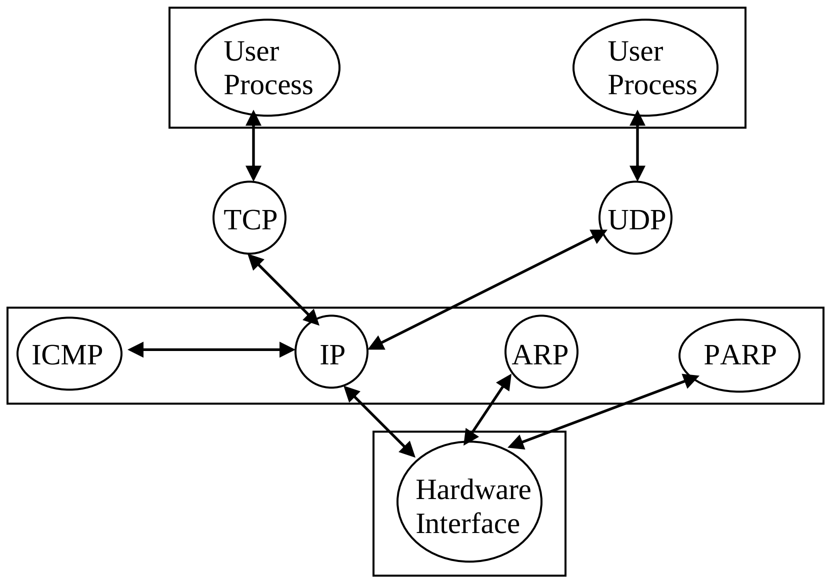
TCP/IP प्रोटोकॉल सूट की कुछ सार्व सुरक्षा कमजोरियां हैं:

- HTTP ट्रांसफर फाइल्स के लिए उपयोग की जाने वाली TCP/IP सूट में एक एप्लीकेशन लेयर प्रोटोकॉल है जो वेब सर्वर से वेब पेज बनाते हैं। ये स्थानांतरण प्लेन–टेक्स्ट (साधारण–पाठ) में किए जाते हैं और एक घुसपैठिया सर्वर और क्लाइंट के मध्य बदले गए डेटा पैकेट को आसानी से पढ़ सकता है।
- एक और HTTP भेद्यता सत्र के आरंभ के दौरान क्लाइंट और वेब सर्वर के मध्य एक कमजोर प्रमाणीकरण है। यह भेद्यता एक सत्र अपहरण हमले का कारण बन सकती है जहाँ हमलावर वैध उपयोगकर्ता का एक HTTP सत्र चुराता है।
- कनेक्शन स्थापना के लिए TCP प्रोटोकॉल भेद्यता तीन–तरफा हैंडशेक है। एक हमलावर इस भेद्यता का लाभ उठाने के लिए सेवा हमले SYN-flooding का खंडन कर सकता है। वह हैंडशेक पूरा नहीं करके आधे–अधूरे सत्रों की स्थापना करता है। इससे सर्वर ओवरलोड हो जाता है और आखिरकार क्रैश हो जाता है।
- IP परत कई कमजोरियों के लिए अतिसंवेदनशील है। IP प्रोटोकॉल हेडर संशोधन के माध्यम से, एक हमलावर IP स्पूफिंग हमला आरंभ कर सकता है।

उपर्युक्त के अतिरिक्त, TCP/IP प्रोटोकॉल परिवार में कई अन्य सुरक्षा कमजोरियाँ उपलब्ध हैं, साथ ही इसके कार्यान्वयन में भी।

संयोग से, TCP/IP आधारित नेटवर्क संचार में, यदि एक परत को हैक किया जाता है, तो दूसरी परतें हैक के बारे में पता नहीं करती हैं और संपूर्ण संचार समझौता हो जाता है। इसलिए, मूर्खतापूर्ण सुरक्षा सुनिश्चित करने के लिए प्रत्येक परत पर सुरक्षा नियंत्रण को नियोजित करने की आवश्यकता है।

TCP/IP प्रोटोकॉल को चार परतों में विभाजित किया जाता है, तथा प्रत्येक परत में एक या एक से अधिक प्रोटोकॉल होते हैं। निम्न चित्र देखें:



प्रत्येक प्रोटोकॉल का कार्य पूर्व निर्धारित होता है जो निम्न है:

(i) TCP (Transmission Control Protocol): यह कनेक्शन ओरिएन्टेड प्रोटोकॉल कहलाता है जो उपयोगकर्त्ता प्रक्रम हेतु विश्वसनीय, फुल डुप्लेक्स तथा डाटा को बाइट स्ट्रीम में स्थानान्तरित करता है। अधिकांशतः इंटरनेट एप्लीकेशन प्रोग्राम इसी प्रोटोकॉल का प्रयोग करते हैं, क्योंकि यह IP प्रोटोकॉल का प्रयोग करता है। अतः इसे TCP/IP प्रोटोकॉल कहते हैं।

(ii) UDP (User Datagram Protocol): यह उपयोगकर्त्ता प्रक्रम के लिए कनेक्शन रहित प्रोटोकॉल है। यह किसी भी प्रकार की निश्चिता प्रदान नहीं करता है कि हमारा डाटाग्राम अपने सुनिश्चित स्थान पर पहुँच जायेगा, जबकि TCP प्रोटोकॉल यह निश्चता प्रदान करता है।

(iii) ICMP (Internet Control Message Protocol): यह गेटवे तथा उपयोगकर्त्ता के मध्य होने वाली त्रुटियों को संभालता है तथा उनके मध्य सूचना के आदान–प्रदान को नियंत्रित करता है। ICMP संदेश IP डाटाग्राम के द्वारा भेजे जाते हैं।

(iv) IP (Internet Protocol): यह TCP, UDP तथा ICMP को डाटा पैकेट पहुँचाने का कार्य करता है।

(v) ARP (Address Resolution Protocol): ये इंटरनेट एड्रेस को हार्डवेयर मशीन पर मानचित्रित करने का कार्य करते हैं।

(vi) RARP (Reverse Address Resolution Protocol): ये हार्डवेयर एड्रेस को इंटरनेट ऐड्रेस पर मानचित्रित करने का कार्य करते हैं।

TCP/IP मॉडल OSI मॉडल का संक्षिप्त संस्करण है। इसमें OSI मॉडल की सात परतों के विपरीत चार परतें शामिल हैं। ये परतें निम्न हैं:

1. प्रक्रिया/अनुप्रयोग परत
2. होस्ट–टू–होस्ट/ट्रांसपोर्ट परत
3. इंटरनेट परत
4. नेटवर्क एक्सेस/लिंक परत

1. नेटवर्क एक्सेस/लिंक परत:

यह परत OSI मॉडल के डेटा लिंक परत और भौतिक परत के संयोजन के संगत होती है। यह हार्डवेयर एड्रेसिंग के लिए दिखता है और इस परत में उपलब्ध प्रोटोकॉल डेटा के भौतिक स्थानान्तरण के लिए अनुमति देता है।

हमने अभी ARP को इंटरनेट परत का एक प्रोटोकॉल होने की बात की थी, लेकिन इसे इंटरनेट परत या नेटवर्क एक्सेस परत के प्रोटोकॉल के रूप में घोषित करने के बारे में एक विरोधाभास है। इसे परत 3 में रहने के रूप में वर्णित किया गया है, परत 2 प्रोटोकॉल द्वारा समझाया जाता है।

2. इंटरनेट परत:

यह परत OSI के नेटवर्क परत के कार्यों को समानता देता है। यह उन प्रोटोकॉल को परिभाषित करता है जो पूरे नेटवर्क पर डेटा के तार्किक संचरण के लिए जिम्मेदार हैं। इस परत पर रहने वाले मुख्य प्रोटोकॉल हैंः

(1) IP – इसका विस्तारित रूप इंटरनेट प्रोटोकॉल है और यह पैकेट हेडर में IP पते को देखकर स्रोत होस्ट से गंतव्य होस्ट को पैकेट पहुंचाने के लिए जिम्मेदार है। IP के 2 संस्करण हैंः IPv4 और IPv6। IPv4 वह है जिनका वर्तमान में अधिकांश वेबसाइट्स उपयोग कर रही हैं। लेकिन IPv6 बढ़ रहा है क्योंकि उपयोगकर्ताओं की संख्या की तुलना में IPv4 पतों की संख्या सीमित है।

(2) ICMP – इसका विस्तारित रूप इंटरनेट कंट्रोल मैसेज प्रोटोकॉल है। यह IP डाटाग्राम के अंदर एनकैप्सुलेटेड है और नेटवर्क समस्याओं के बारे में जानकारी प्रदान करने के लिए मेजबान को प्रदान करने के लिए जिम्मेदार है।

(3) ARP – इसका विस्तारित रूप एड्रेस रिजॉल्यूशन प्रोटोकॉल है। इसका काम एक ज्ञात IP पते से होस्ट का हार्डवेयर पता ढूंढना है। ARP के कई प्रकार होते हैंः उत्क्रम ARP, परोक्षी (Proxy ARP), ऐच्छिक (Gratuitous ARP) और व्युत्क्रम (Inverse) ARP।

3. होस्ट–टू–होस्ट/ट्रांसपोर्ट परत:

यह परत OSI मॉडल की ट्रांसपोर्ट परत के अनुरूप है। यह अंत–से–अंत संचार और डेटा की त्रुटि–मुक्त वितरण के लिए उत्तरदायी है। यह डेटा की जटिलताओं से ऊपरी–परत अनुप्रयोगों को ढालता है। इस परत में उपलब्ध दो मुख्य प्रोटोकॉल हैंः

(1) TCP – इसका विस्तारित रूप ट्रांसमिशन कंट्रोल प्रोटोकॉल है। यह अंत–से–अंत प्रणाली के मध्य विश्वसनीय और त्रुटि रहित संचार प्रदान करने के लिए जाना जाता है। यह डेटा का अनुक्रमण और विभाजन करता है। इसमें पावती सुविधा भी है और प्रवाह नियंत्रण तंत्र के माध्यम से डेटा के प्रवाह को नियंत्रित करता है। यह एक बहुत ही प्रभावी प्रोटोकॉल है, लेकिन इस तरह की विशेषताओं के कारण बहुत अधिक ओवरहेड है। ओवरहेड बढ़ने से लागत में वृद्धि होती है।

(2) UDP – इसका विस्तारित रूप यूजर डेटाग्राम प्रोटोकॉल है। दूसरी ओर ऐसी कोई भी सुविधा प्रदान नहीं करता है। यह go-to प्रोटोकॉल है, यदि हमारे एप्लीकेशन को विश्वसनीय परिवहन की आवश्यकता न हो, क्योंकि यह बहुत ही लागत प्रभावी है। TCP के विपरीत, जो कनेक्शन–उन्मुख प्रोटोकॉल होता है, UDP कनेक्शन रहित है।

4. प्रक्रिया/अनुप्रयोग परत:

यह परत OSI मॉडल की शीर्ष तीन परतों का कार्य करती हैः अनुप्रयोग, प्रस्तुति और सत्र परत। यह नोड–टू–नोड संचार के लिए उत्तरदायी है और उपयोगकर्ता–इंटरफेस विनिर्देशों को नियंत्रित करता है। इस परत में उपलब्ध कुछ प्रोटोकॉल हैंः HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD। इनमें से कुछ प्रोटोकॉल के बारे में नीचे विस्तारित किया गया है।

HTTP और HTTPS – HTTP का अर्थ हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल है। इसका उपयोग वर्ल्ड वाइड वेब द्वारा वेब ब्राउजर और सर्वर के मध्य संचार का प्रबंधन करने के लिए किया जाता है। HTTPS का अर्थ HTTP-Secure है। यह HTTP के साथ SSL (Secure Socket Layer) का संयोजन है। यह उन दशाओं में कुशल है जहाँ ब्राउजर को फॉर्म भरने, साइन इन (sign in) करने, प्रमाणित करने और बैंक लेनदेन करने की आवश्यकता होती है।

SSH – इसका विस्तारित रूप Secure Shell है। यह टेलनेट के समान एक टर्मिनल एमुलेशन सॉफ्टवेयर है। SSH अधिक पसंद किया जाता है इसका कारण एन्क्रिप्टेड कनेक्शन को बनाए रखने की क्षमता है। यह TCP/IP कनेक्शन पर एक सुरक्षित सत्र व्यवस्थित करता है।

NTP – इसका विस्तारित रूप नेटवर्क टाइम प्रोटोकॉल है। इसका उपयोग हमारे कम्प्यूटर पर घड़ियों को एक मानक समय स्रोत में सिन्क्रोनाइज करने के लिए किया जाता है। यह बैंक लेनदेन जैसी स्थितियों में बहुत उपयोगी है। NTP की उपस्थिति के बिना निम्न स्थिति को लेंः माना हम एक लेन–देन करते हैं, जहाँ हमारा कम्प्यूटर दोपहर 2:30 बजे पढ़ता है, जबकि सर्वर इसे 2:28 बजे रिकॉर्ड करता है। यदि यह सिंक से बाहर है तो सर्वर बहुत बुरी तरह से दुर्घटनाग्रस्त हो सकता है।

FTP (File Transfer Protocol):

फाइलों को एक सिस्टम से दूसरे सिस्टम पर स्थानान्तरित करने के लिए इस प्रोटोकॉल का प्रयोग किया जाता है। यह कई विकल्प प्रदान करता है, जैसे यूजर ऑथैंटिकेशन, डाटा स्थानान्तरण, डायरेक्ट्री की सूची आदि। जब उपयोगकर्त्ता अपने सिस्टम पर FTP क्लाइंट प्रोसेस का आरंभ करता है, तब यह क्लाइंट प्रोसेस TCP प्रोटोकॉल की सहायता से FTP रिमोट सर्वर के साथ कनेक्शन स्थापित करता है। FTP दो प्रकार के कनेक्शन स्थापित करता है। प्रथम कनेक्शन क्लाइंट और सर्वर के मध्य कमांड तथा उसका परिणाम देने हेतु एवं दूसरा कनेक्शन डाटा का स्थानान्तरण करने के लिए। यह प्रोटोकॉल बाइनरि तथा टेकस्ट फाइल्स का आदान–प्रदान करता है।

TFTP (Trivial File Transfer Protocol):

इसका उपयोग क्लाइंट तथा सर्वर प्रोसेस के मध्य फाइल्स के आदान–प्रदान करने के लिए किया जाता है। यह UDP प्रोटोकॉल का प्रयोग करता है न कि TCP का। इसकी सहायता से किसी भी वर्कस्टेशन को LAN में आसानी से जोड़ा जा सकता है तथा ROM में आसानी से कार्यान्वित किया जा सकता है।

TELNET: यह रिमोट लॉग–इन की सुविधा प्रदान करता है। यह FTP के समान TCP प्रोटोकॉल का उपयोग करता है। इसका मानक प्रोग्राम RFC854 [Postel और Reynolds 1983] है।

5. SMTP (Simple Mail Transfer Protocol):

दो सिस्टम के मध्य मेल का आदान–प्रदान करने के लिए इस प्रोटोकॉल का प्रयोग किया जाता है। इसकी परिभाषा RFC821 [Postel 1982] है।

6. XNS (Xerox Network System):

इसे जीरॉक्स कार्पोरेशन ने 1970 में निर्मित किया था। अधिकांशतः 4.3 BSD सिस्टम XNS को सपोर्ट करते हैं। इस प्रोटोकॉल की संरचना TCP/IP प्रोटोकॉल के समान होती है। इस प्रोटोकॉल में चार परतें होती हैं तथा प्रत्येक परत में एक से अधिक प्रोटोकॉल होते हैं। अतः इसे XNS प्रोटोकॉल सूट भी कहते हैं। XNS की विभिन्न परतों में प्रयुक्त प्रोटोकॉल निम्न हैं:

(i) ECHO (Echo Protocol): यह उस पैकेट के बारे में बताता है जो कि होस्ट ने प्राप्त किया है। अधिकतर XNS प्रोटोकॉल में इस प्रोटोकॉल का प्रयोग किया जाता है।

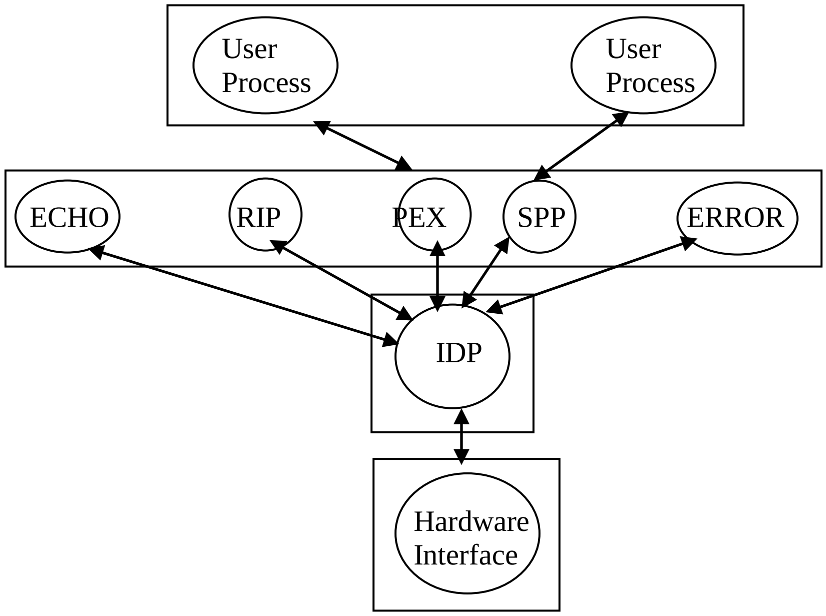
(ii) RTP (Routing Information Protocol): यह उस रॉउटिंग डाटाबेस को बनाए रखता है जो एक होस्ट से IDP पैकेट के रूप में दूसरे होस्ट तक भेजे जाते हैं। एक होस्ट से दूसरे होस्ट तक भेजे जाने वाले पैकेटों के पथ की जानकारी रखने का कार्य RIP प्रोटोकॉल करता है।

(iii) PEX (Packet Exchange Protocol): यह उपयोगकर्त्ता प्रक्रम के लिए कनेक्शन रहित प्रोटोकॉल है। यह किसी भी प्रकार की निश्चिता प्रदान नहीं करता है कि हमारा डाटाग्राम अपने सुनिश्चित स्थान पर पहुँच जायेगा, जबकि TCP प्रोटोकॉल यह निश्चता प्रदान करता है। यह प्रोटोकॉल सिर्फ ट्रॉन्समिशन करता है।

(iv) ERRORP (Error Protocol): किसी भी प्रकार के प्रक्रम में इस प्रोटोकॉल का प्रयोग किया जाता है। यदि किसी भी प्रक्रम को डाटा ट्रॉन्समिशन में कोई त्रुटि मिलती है तो उस त्रुटि की रिपोर्ट इस प्रोटोकॉल को की जाती है।

(v) IDP (Internet Datagram Protocol): यह कनेक्शन रहित प्रोटोकॉल है। यह किसी भी प्रकार की निश्चिता प्रदान नहीं करता है कि हमारा डाटाग्राम अपने सुनिश्चित स्थान पर पहुँच जायेगा। यह डाटा को डाटाग्राम के रूप में भेजता है। यह प्रोटोकॉल ऊपर की सभी परतों को पैकेट पहुँचाने का कार्य करता है।

7. UUCP (Unix to Unix Copy Protocol):



यह कई प्रोग्राम्स का एक समूह होता है। यह फाइल्स को कॉपी करने तथा कमाण्ड को दूसरे सिस्टम पर रन करने का कार्य करता है। इस प्रोटोकॉल का प्रथम संस्करण Version 7 Unix के नाम से 1978 में निर्मित किया गया था जो टेलीफोन लाइन की सहायता से डॉयल–अप नेटवर्क पर कार्य करता था। वर्तमान में इसके दो संस्करण मौजूद हैं। UUCP प्रोटोकॉल कई प्रोग्राम्स का एक समूह होता है, उनमें से कुछ प्रोग्राम निम्न हैंः

(i) UUCP: किसी भी फाइल को एक सिस्टम से दूसरे सिस्टम पर कॉपी करने के लिए इसका प्रयोग किया जाता है। यह यूनिक्स के cp कमांड पर आधारित होता है, जिसका कार्य एक से अधिक फाइलों को कॉपी करना है।

(ii) UUX: यह प्रोग्राम कई कमांड्स को रखता उपयोगकर्त्ता इन कमांड्स को अधिकतर उपयोग में लाता है।

(iii) UUCICO: यह प्रोग्राम तब रन होता है जब कोई प्रक्रम उस कार्य को करने का आग्रह करता है जो कि UUCP या UUX द्वारा पहले भेजी गयी कमान्ड्स के द्वारा संभव नहीं है।

(iv) UUXQT: यह उन फाइलों को रन करने का कार्य करता है जो UUX प्रोग्राम द्वारा प्रदान की जाती है। इसे अधिकांशतः UUX द्वारा सक्रिय किया जाता है ताकि यह उन फाइल्स को रन कर सके जो कि दूसरे सिस्टम से प्राप्त की गई हैं।

TCP/IP के लाभः

TCP/IP अप्रसारक है और परिणामस्वरूप, किसी एक कंपनी द्वारा नियंत्रित नहीं किया जाता है। इसलिए, इंटरनेट प्रोटोकॉल सूट को आसानी से संशोधित किया जा सकता है। यह सभी ऑपरेटिंग सिस्टम के साथ संगत है, इसलिए यह किसी अन्य सिस्टम के साथ संचार कर सकता है। इंटरनेट प्रोटोकॉल सूट सभी प्रकार के कम्प्यूटर हार्डवेयर और नेटवर्क के साथ भी संगत है।

TCP/IP मॉडल का गुणः

1. यह स्वतंत्र रूप से संचालित होता है।
2. यह स्केलेबल है।
3. क्लाइंट/सर्वर आर्किटेक्चर।
4. कई रूटिंग प्रोटोकॉल का समर्थन करता है।
5. दो कम्प्यूटर्स के मध्य संबंध स्थापित करने के लिए इस्तेमाल किया जा सकता है।

TCP/IP के दोषः
1. यह ट्रांसपोर्ट लेयर पैकेट के वितरण का आश्वासन नहीं देता है।
2. मॉडल का उपयोग किसी अन्य एप्लिकेशन में नहीं किया जा सकता है।
3. प्रोटोकॉल को बदलना आसान नहीं है।
4. इसने अपनी सेवाओं, इंटरफेस और प्रोटोकॉल को स्पष्ट रूप से अलग नहीं किया है।

TCP/IP मॉडल और OSI मॉडल का तुलनात्मक अध्ययनः

TCP/IP मॉडल और OSI मॉडल का तुलनात्मक अध्ययन करने के पूर्व हमें OSI मॉडल को समझाना होगा।

OSI मॉडल की परिभाषाः

अंतर्राष्ट्रीय मानक संगठन (ISO) द्वारा ओपन सिस्टम इंटरकनेक्शन (OSI) मॉडल प्रस्तुत किया गया था। यह एक प्रोटोकॉल नहीं है बल्कि एक मॉडल है जो परत की अवधारणा पर आधारित है। इसमें परतों का एक ऊर्ध्वाधर समूह होता है, प्रत्येक में अलग–अलग कार्य होते हैं। यह डेटा को स्थानांतरित करने के लिए बॉटम–अप दृष्टिकोण का अनुसरण करता है। यह मजबूत और लचीला है, लेकिन ठोस नहीं है।

OSI संदर्भ मॉडल का मुख्य उद्देश्य डिजिटल संचार हार्डवेयर, उपकरणों और सॉफ्टवेयर के डिजाइन और विकास का संचालन करना है, ताकि वे कुशलता से हस्तक्षेप कर सकें।

OSI मॉडल की सात परतें निम्न हैंः

1. अनुप्रयोग परत – इस परत के साथ, उपयोगकर्ता इलेक्ट्रॉनिक मेल, साझा डेटाबेस प्रबंधन, फाइल एक्सेस/ट्रांसफर और अन्य सेवाओं जैसे इंटरफेस और सेवाओं का उपयोग करके नेटवर्क तक पहुंच सकते हैं।
2. प्रस्तुतिकरण परत – प्रस्तुतिकरण परत ट्रांसमिटिंग इंफॉर्मेशन के सिंटैक्स और शब्दार्थ पर केंद्रित है। यह अनुवाद, एन्क्रिप्शन और कम्प्रेशन जैसे कार्य करता है जहाँ कैरेक्टर स्ट्रिंग, संख्या, प्रतीकों के रूप में विद्यमान वास्तविक जानकारी को बिट स्ट्रीम में एनकोड किया जाता है, जिसे दूसरे रूप में परिवर्तित किया जाता है और संपीड़ित किया जाता है।
3. सत्र परत – यह परत अलग–अलग मशीनों के मध्य सत्र को स्थापित करती है ताकि उनके मध्य बातचीत को सिन्क्रोनाइज और बनाए रखा जा सके। सत्र परत द्वारा प्रदान की जाने वाली सेवाएं संवाद नियंत्रण, टोकन प्रबंधन और सिन्क्रोनाइजेशन हैं।
4. परिवहन परत – यह स्वतंत्र पैकेट के रूप में अपनी पूर्ववर्ती परत से डेटा को स्वीकार करता है और इसे उचित क्रम में सफल परत तक पहुँचाता है। इस परत द्वारा किए गए अन्य कार्य सेवा बिंदु पते, कनेक्शन नियंत्रण, विभाजन और पुनः विकास, प्रवाह नियंत्रण और त्रुटि नियंत्रण हैं।
5. नेटवर्क परत – लॉजिकल एड्रेसिंग और राउटिंग नेटवर्क परत द्वारा किए जाने वाले प्रमुख ऑपरेशन हैं। यह नेटवर्क MAC पते को भौतिक MAC पते में बदल देता है ताकि विभिन्न नेटवर्क में रहने वाले दो सिस्टम भी कुशलता से संवाद कर सकें। एक पैकेट को भी भीड़ और असफल घटकों से बचने के लिए गंतव्य तक पहुँचने हेतु एक मार्ग की आवश्यकता होती है, इसलिए यह मार्गों के स्वचालित अद्यतन की सुविधा भी प्रदान करता है।
6. डेटा लिंक परत – यह कच्चे ट्रांसमिशन सेवा (भौतिक परत) को एक विश्वसनीय लिंक में बदलने के लिए उत्तरदायी है। यह भौतिक परत को उन्हें मास्क करके त्रुटि से मुक्त बनाता है ताकि नेटवर्क परत उन्हें नोटिस न करें। इस परत में, इनपुट डेटा को फ्रेम में विभाजित किया जाता है। डेटा लिंक परत में किए गए कार्य फ्रेमिंग, एक्सेस कंट्रोल, फिजिकल एड्रेसिंग, एरर और फ्लो कंट्रोल हैं।
7. भौतिक परत – यह ट्रांसमिशन चैनल पर व्यक्तिगत बिट्स को प्रसारित करता है। भौतिक परत उपकरणों और ट्रांसमिशन मीडिया, बिट्स का प्रतिनिधित्व, बिट्स का सिन्क्रोनाइजेशन, डेटा दर, भौतिक टोपोलॉजी, लाइन कॉन्फिगरेशन, ट्रांसमिशन मोड के मध्य इंटरफेस की विशेषताओं का वर्णन करती है।

TCP/IP और OSI मॉडल के मध्य मुख्य अंतर निम्न हैंः

1. TCP/IP एक क्लाइंट–सर्वर मॉडल है, अर्थात जब क्लाइंट सेवा के लिए अनुरोध करता है तो यह सर्वर द्वारा प्रदान किया जाता है। जबकि, OSI एक वैचारिक मॉडल है।
2. TCP/IP एक मानक प्रोटोकॉल है जिसका उपयोग इंटरनेट सहित हर नेटवर्क के लिए किया जाता है, जबकि, OSI एक प्रोटोकॉल नहीं है, बल्कि सिस्टम आर्किटेक्चर को समझने और डिजाइन करने के लिए उपयोग किया जाने वाला एक संदर्भ मॉडल है।
3. TCP/IP एक चार–स्तरित मॉडल है, जबकि OSI में सात परतें हैं।
4. TCP/IP ऊर्ध्वाधर दृष्टिकोण का अनुसरण करता है। दूसरी ओर, OSI मॉडल क्षैतिज दृष्टिकोण का समर्थन करता है।
5. TCP/IP मूर्त है, जबकि, OSI नहीं है।
6. TCP/IP शीर्ष से नीचे के दृष्टिकोण का अनुसरण करता है, जबकि, OSI मॉडल बॉटम–अप दृष्टिकोण का अनुसरण करता है।

नीचे दिए गए आरेख तुलना के साथ, OSI संदर्भ मॉडल और TCP/IP संदर्भ मॉडल के मध्य कुछ प्रमुख अंतर को दर्शाते हैंः

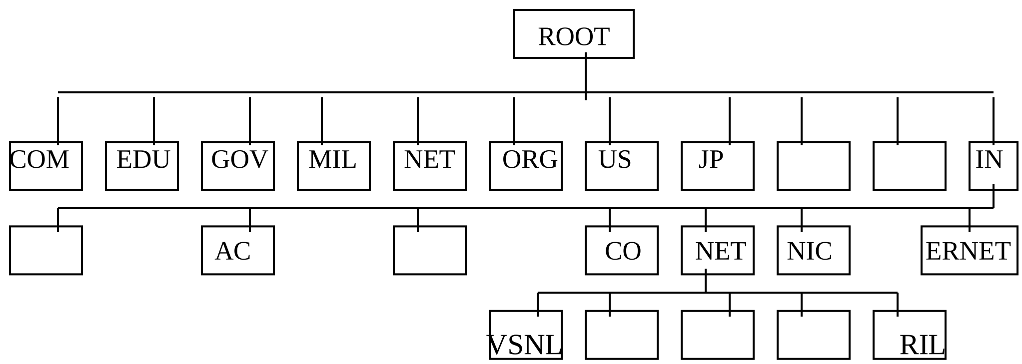
ओपन सिस्टम इंटरकनेक्शन (OSI)	ट्रांसमिशन कंट्रोल प्रोटोकॉल/ इंटरनेट प्रोटोकॉल (TCP/IP)
OSI एक सामान्य, प्रोटोकॉल स्वतंत्र मानक है, जो नेटवर्क और अंतिम उपयोगकर्ता के मध्य संचार द्वार के रूप में कार्य करता है।	TCP/IP मॉडल मानक प्रोटोकॉल पर आधारित है जिसके आसपास इंटरनेट विकसित हुआ है। यह एक संचार प्रोटोकॉल है, जो एक नेटवर्क पर मेजबानों के कनेक्शन की अनुमति देता है।
OSI मॉडल में ट्रांसपोर्ट परत पैकेट की डिलीवरी का आश्वासन देता है।	TCP/IP मॉडल में परिवहन परत पैकेट वितरण का आश्वासन नहीं देता है। अभी भी TCP/IP मॉडल अधिक विश्वसनीय है।
ऊर्ध्वाधर दृष्टिकोण का अनुसरण करता है।	क्षैतिज दृष्टिकोण का अनुसरण करता है।
OSI मॉडल में एक पृथक प्रस्तुति परत और सत्र परत है।	TCP/IP मॉडल पृथक से प्रस्तुति परत और सत्र परत नहीं रखता है।
ट्रांसपोर्ट परत कनेक्शन उन्मुख होता है।	ट्रांसपोर्ट परत कनेक्शन उन्मुख और कनेक्शन रहित दोनों होता है।
नेटवर्क परत कनेक्शन उन्मुख और कनेक्शन रहित दोनों होता है।	नेटवर्क परत कनेक्शन रहित होता है।
OSI एक संदर्भ मॉडल है जिसके चारों ओर नेटवर्क बनाए जाते हैं। आम तौर पर इसका उपयोग एक मार्गदर्शन उपकरण के रूप में किया जाता है।	TCP/IP मॉडल, एक प्रकार से OSI मॉडल का एक कार्यान्वयन है।
OSI मॉडल में प्रोटोकॉल को मॉडल में व्यवस्थित करने की समस्या है।	TCP/IP मॉडल किसी भी प्रोटोकॉल को व्यवस्थित नहीं करता है।
प्रोटोकॉल OSI मॉडल में छिपे हुए हैं और प्रौद्योगिकी के परिवर्तन के रूप में आसानी से बदल दिए जाते हैं।	TCP/IP मॉडल में प्रोटोकॉल को बदलना आसान नहीं है।
OSI मॉडल सेवाओं, इंटरफेस और प्रोटोकॉल को बहुत स्पष्ट रूप से परिभाषित करता है और उनके मध्य स्पष्ट अंतर करता है। यह प्रोटोकॉल स्वतंत्र है।	TCP/IP में, सेवाओं, इंटरफेस और प्रोटोकॉल स्पष्ट रूप से पृथक नहीं होते हैं। यह प्रोटोकॉल पर निर्भर भी है।
यह सात परत रखता है।	यह चार परत रखता है।

8.2.2 DNS प्रोटोकॉल (संदेशाचार):

डोमेन नेम सिस्टम (DNS) का उपयोग होस्ट डोमेन नाम को IP पतों पर हल करने के लिए किया जाता है। नेटवर्क उपयोगकर्ता मुख्य रूप से वेब ब्राउजर में URL लिखकर इंटरनेट ब्राउजिंग के दौरान DNS कार्यक्षमता पर निर्भर करते हैं।

DNS पर एक हमले में, एक हमलावर का उद्देश्य एक वैध DNS रिकॉर्ड को संशोधित करना है ताकि यह एक गलत IP पते पर हल हो जाए। यह उस आईपी के लिए सभी ट्रैफिक को गलत कम्प्यूटर पर निर्देशित कर सकता है। एक हमलावर या तो DNS प्रोटोकॉल भेद्यता का शोषण कर सकता है या एक हमले को लागू करने के लिए DNS सर्वर से समझौता कर सकता है।

DNS कैश पॉइजनिंग डीएनएस प्रोटोकॉल में पाई जाने वाली भेद्यता का शोषण करने वाला हमला है। एक हमलावर एक रिहायशी द्वारा भेजे गए पुनरावर्ती DNS क्वेरी के लिए एक प्रतिक्रियाशील फोर्जिंग करके कैश को समाप्त सकता है जो एक आधिकारिक सर्वर पर है। एक बार, DNS रिजॉल्वर के कैश को समाप्त कर दिया जाता है, मेजबान एक दुर्भावनापूर्ण वेबसाइट को निर्देशित करेगा और इस साइट पर संचार द्वारा विश्वसनीय जानकारी से समझौता कर सकता है।



किसी व्यक्ति या शहर के नाम के समान इंटरनेट से जुड़े हुए कम्प्यूटर्स को भी डोमेन नाम प्रणाली के अंतर्गत शब्दों में नाम प्रदान किए जाते हैं, ताकि उस कम्प्यूटर की स्थिति को जाना जा सके। इंटरनेट से जुड़े प्रत्येक होस्ट कम्प्यूटर का एक डोमेन नाम अव य होता है। इन शब्दों से बने डोमेन नाम के समानान्तर ही इन कम्प्यूटर्स को एक अंको पर आधारित इंटरनेट प्रोटोकॉल पता (IP Address) भी दिया जाता है, अर्थात् इंटरनेट से जुड़े हुए प्रत्येक होस्ट कम्प्यूटर का एक डोमेन नाम व इंटरनेट प्रोटोकॉल पता अवश्य होता है।

डोमेन नाम की सहायता से किसी भी कम्प्यूटर के संस्थान व उसकी भौतिक स्थिति का पता लगता है, अर्थात् वह कम्प्यूटर किस देश का है, किस संस्थान का है व वह किस प्रकार का है इसका अनुमान सरलता से लग जाता है। डोमेन नाम को समझने के लिए हम निम्न उदाहरण को लेते हैं:

माना barc.res.rnet.in

किसी कम्प्यूटर का डोमेन नाम है। इसे निम्न प्रकार दायीं ओर से समझा जा सकता है:

1. यह .in अर्थात् INDIA में स्थित है।
2. यह rnet अर्थात् रिसर्च नेटवर्क के अंतर्गत है।
3. यह res अर्थात् रिसर्च से संबंधित है।
4. इस कम्प्यूटर का नाम BARC है, जो संभवतः किसी संस्थान का नाम है।

इंटरनेट के अंतर्गत 6 ऐसे भी डोमेन है जो भौगोलिक स्थिति पर आधारित नहीं है। अर्थात् इनके साथ देश का कोड नहीं लगा है। वे निम्न हैं:

.com	वाणिज्यिक संस्थानों के लिए।
.edu	शिक्षा संस्थानों के लिए।
.gov	शासकीय संस्थानों के लिए।
.mil	सैन्य संस्थानों के लिए।

.net	इंटरनेट के अंदर ही अन्य नेटवर्क संस्थानों के लिए।
.org	उन संस्थानों के लिए जो न तो वाणिज्यिक और न ही शिक्षा में आते हैं।

टीपः **.**com, **.**edu, **.**gov डोमेन अमेरिका स्थित हैं। अमेरिकन डोमेन में **.**us देश का नाम नहीं लगाते हैं। अर्थात् जहाँ देश का नाम **.**in, **.**au, **.**uk नहीं होता वह सर्वर अमेरिका स्थित है।

IP पता प्रणालीः

IP पता प्रणाली के अंतर्गत इंटरनेट से जुड़े समस्त होस्ट कम्प्यूटर्स को अंकों के एक समूह का उपयोग करते हुए अलग–अलग ऑक्टेल संख्या प्रदान किया जाता है, यहाँ ऑक्टेल अंकों का समूह उस कम्प्यूटर का IP पता कहलाता है। जब किसी कम्प्यूटर से डाटा का आदान–प्रदान करने के लिए हम डोमेन नाम प्रणाली के अनुसार उस कम्प्यूटर का इंटरनेट पता शब्दों में अपने कम्पयूटर को देते हैं तो हमारा सर्वर कम्प्यूटर इस पते को IP पते में अर्थात् निर्धारित अंकों में परिवर्तित करता है। इसके उपरान्त ही कनेक्शन की प्रक्रिया आगे बढ़ती है। इंटरनेट से जुड़े हुए प्रत्येक कम्प्यूटर का अलग–अलग IP पता अर्थात् नम्बर होता है।

IP पते के चार भाग होते हैं और ये सभी भाग डॉट (**.**) द्वारा एक दूसरे से जुड़े होते हैं। उदाहरण के लिए दिल्ली स्थित VSNL सर्वर के IP पते को लेंः 202.54.15.1

टीपः

IP पते को सदैव बायीं ओर से दायीं ओर तथा डोमेन नाम को दायीं ओर से बायीं ओर पढ़ा जाता है। यहाँ 202.54.15.1 भारत के VSNL को दिया गया IP पता है जिसे हम निम्न प्रकार पढ़ेंगेः

202.54	in.net
15	vsnl
1	दिल्ली स्थित सर्वर

1 से 254 तक का अंक प्रदान कर VSNL द्वारा देश में कुल 254 सर्वर स्थापित किया जा सकता है। इस IP पता प्रणाली को निम्न टेलीफोन नम्बर द्वारा सरलता से समझा जा सकता है, माना किसी अन्य देश में बैठा कोई व्यक्ति भोपाल में 2761419 फोन नम्बर पर वार्ता करना चाहता है, तो उसे 0091 0755 2761419 डॉयल करना होगा, अर्थात् सर्वप्रथम भारत का कोड 0091, तत्पश्चात भोपाल का कोड 0755 और फिर वांछित नम्बर 276149। इसी प्रकार इंटरनेट पर भी वांछित कम्प्यूटर तक पहुँचने के लिए IP पते में सर्वप्रथम उसकी भौगोलिक स्थिति अनुसार कोड, तत्पश्चात नेटवर्क का कोड, इसके उपरांत संस्थान का कोड फिर वांछित कोड टाइप करना होगा।

डोमेन नाम का पंजीकरणः

IP पता एवं डोमेन नाम प्रदाय करने का कार्य IANA (इंटरनेट असाइंड नम्बर अथॉरिटि) नामक प्राधिकरण INTERNIC (इंटरनेट नेटवर्क इनफारमेशन सेंटर) के द्वारा करता है।

यदि हम INTERNIC से अपने डोमेन नाम का पंजीकरण करवाना चाहते हैं तब हमें वर्तमान दर से INTERNIC को भुगतान करना होगा। इसके पश्चात हमारा डोमेन नाम 2 वर्षों के लिए पंजीकृत हो जाता है, तथा डोमेन नाम के अंत में **.**com, **.**edu या **.**org लगा होगा।

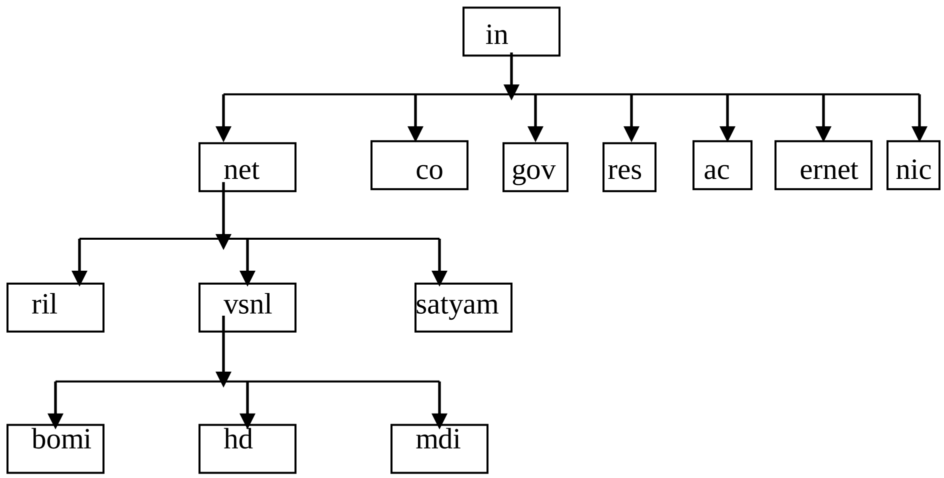
लेकिन यदि हम भारत में डोमेन नाम पंजीकृत करवाना चाहते हैं, तो हमें भारत के लिए निर्धारित क्षेत्रीय पंजीकरण इकाई NCST (नेशनल सेंटर फॉर सॉफ्टवेयर टेक्नॉलाजी) मुम्बई को आवेदन करना होगा। प्रदाय किए गए डोमेन नाम के अंत में **.**in लगा होगा। IN डोमेन के अंतर्गत द्वितीय स्तर पर सब–डोमेन के रूप में ERNET (Education & Research NET) शैक्षणिक एवं खोज संस्थाओं हेतु, NIC-नेशनल इनफारमेटिक्स सेंटर हेतु NET-इंटरनेट सर्विस प्रोवाइडर हेतु आदि डोमेन हैं।

तृतीय स्तर के डोमेन के रूप में वह संस्थान जिसके लिए डोमेन नाम प्रदाय किया जा रहा है के नाम का उपयोग किया जाता है। उदाहरण के लिए 'vsnl.net.in'

यदि हम अपने संस्थान के लिए डोमेन नाम का पंजीकरण कराना चाहते हैं, तो हम आवश्यक आवेदन पत्र domainreg@sangam.ncst.ernet.in से इलेक्ट्रॉनिक विधि से मेल भेज कर प्राप्त कर सकते हैं। आवेदन पत्र को पूरी तरह से भरकर वापस उपरोक्त पते पर ही भेजना होता है। यदि हम समस्त आवश्यक अर्हताऐं पूर्ण करते हैं, तो NCST हमारे डोमेन नाम का पंजीकरण कर लेता है।

भारतीय सर्वरः

net.in	नेटवर्क सुविधा उपलब्ध कराने वाले संस्थानों हेतु
co.in	व्यवसायिक संस्थानों हेतु
gov.in	शासकीय संस्थानों हेतु
res.in	रिसर्च संस्थानों हेतु
ac.in	शैक्षणिक संस्थानों हेतु



DNS प्रोटोकॉल आमतौर पर TCP की तुलना में अपने छोटे ओवरहेड के कारण परिवहन के साधन के रूप में UDP प्रोटोकॉल का उपयोग करता है, यह कम उपरि प्रोटोकॉल है।

DNS प्रोटोकॉल अपनी सेवा के लिए पोर्ट 53 का उपयोग करता है। इसका अर्थ है कि एक DNS सर्वर पोर्ट 53 पर सुनता है और किसी भी क्लाइंट को उसी पोर्ट का उपयोग करने के लिए सेवा का उपयोग करने की उम्मीद करता है। हालाँकि, ऐसी दशायें हैं जहाँ हमें एक भिन्न पोर्ट का उपयोग करने की आवश्यकता हो सकती है, जो हमारे द्वारा चलाए जा रहे ऑपरेटिंग सिस्टम और DNS सर्वर के आधार पर कुछ संभव है।

DNS प्रोटोकॉल में विभिन्न प्रकार के DNS संदेश होते हैं जो उनके संदेश क्षेत्रों में डेटा के अनुसार प्रगति होते हैं। DNS प्रोटोकॉल में संदेश का एक प्रकार होता है जिसमें क्वेरीज होती हैं, अद्यतन, और प्रतिक्रियाएँ, DNS क्वेरी संदेश प्रारूप की लंबाई निर्धारित है जो 12 बाइट्स है।

DNS हेडर की लंबाई और अन्य सभी जैसे प्रश्न प्रविष्टियाँ, उत्तर संसाधन रिकॉर्ड, प्राधिकरण संसाधन रिकॉर्ड, अतिरिक्त संसाधन रिकॉर्ड चर लंबाई है। कई अन्य प्रकार के DNS संदेश या प्रोटोकॉल जैसे DNS क्वेरी संदेश हेडर, DNS क्वेरी प्रश्न प्रविष्टियाँ, DNS संसाधन रिकॉर्ड, नाम क्वेरी संदेश, नाम क्वेरी प्रतिक्रिया, रिवर्स नाम क्वेरी संदेश, DNS अपडेट संदेश प्रारूप, DNS अद्यतन संदेश झंडे, गतिशील अद्यतन प्रतिक्रिया संदेश।

8.2.3 ICMP प्रोटोकॉल (संदेशाचार):

इंटरनेट कंट्रोल मैनेजमेंट प्रोटोकॉल (ICMP) TCP/IP नेटवर्क का एक बुनियादी नेटवर्क प्रबंधन प्रोटोकॉल है। इसका उपयोग नेटवर्क उपकरणों की स्थिति के संबंध में त्रुटि और नियंत्रण संदेश भेजने के लिए किया जाता है।

ICMP, IP नेटवर्क कार्यान्वयन का एक अभिन्न अंग है और इस प्रकार बहुत नेटवर्क सेटअप में उपलब्ध है। ICMP की अपनी कमियाँ हैं और नेटवर्क पर हमले शुरू करने के लिए इसका दुरुपयोग किया जा सकता है।

ICMP कमियों के कारण नेटवर्क पर होने वाले सामान्य हमले निम्न हैं:

- ICMP एक हमलावर को नेटवर्क टोपोलॉजी और नेटवर्क में पथ का निर्धारण करने के लिए नेटवर्क टोही ले जाने की अनुमति देता है। ICMP स्वीप में उन सभी होस्ट IP पतों की खोज करना सम्मिलित है जो पूरे लक्ष्य के नेटवर्क में जीवित हैं।
- ट्रेस मार्ग एक लोकप्रिय ICMP उपयोगिता है जो क्लाइंट से दूरस्थ होस्ट के लिए वास्तविक समय में पथ का वर्णन करके लक्ष्य नेटवर्किंग को मैप करने के लिए उपयोग किया जाता है।
- एक हमलावर ICMP भेद्यता का उपयोग करके सेवा हमले से इनकार कर सकता है। इस हमले में IPMP पिंग पैकेट भेजना सम्मिलित है जो लक्ष्य डिवाइस पर 65,535 बाइट्स से अधिक है। लक्ष्य कम्प्यूटर इस पैकेट को ठीक से संभालने में विफल रहता है और ऑपरेटिंग सिस्टम को कुचलने का कारण बन सकता है।

अन्य प्रोटोकॉल जैसे ARP, DHCP, SMTP आदि की भी अपनी कमियाँ हैं जिनका उपयोग हमलावर द्वारा नेटवर्क सुरक्षा से समझौता करने के लिए किया जा सकता है। प्रोटोकॉल के डिजाइन और कार्यान्वयन के दौरान सुरक्षा पहलू के लिए कम से कम चिंता नेटवर्क सुरक्षा के लिए खतरों का एक मुख्य कारण बन गया है।

ICMP एक त्रुटि रिपोर्टिंग प्रोटोकॉल है जो IP प्रोटोकॉल का एक अभिन्न अंग है। ICMP पूरे नेटवर्क में नियंत्रण डेटा, सूचना डेटा और त्रुटि पुनर्प्राप्ति डेटा का संचार करता है। ट्रांसमिशन त्रुटियों की तुलना में कम गंभीर समस्याएं होने के कारण त्रुटि की स्थिति उत्पन्न हो सकती है। उदाहरण के लिए, मान लीजिए कि इंटरनेट के कुछ भौतिक मार्ग विफल हो जाते हैं, जिससे इंटरनेट को दो नेटवर्क समूह में विभाजित किया जा सकता है, जिसमें समूहों के मध्य कोई रास्ता नहीं है। होस्ट से एक समूह में भेजे गए डेटाग्राम को दूसरे में होस्ट करने के लिए वितरित नहीं किया जा सकता है।

TCP/IP सूट में ICMP नामक एक प्रोटोकॉल सम्मिलित होता है जो IP का उपयोग त्रुटि संदेश भेजने के लिए करता है जब ऊपर वर्णित स्थिति जैसे होती है। IP के एक मानक कार्यान्वयन के लिए प्रोटोकॉल आवश्यक है। हम देखेंगे कि दो प्रोटोकॉल सह–निर्भर हैं। IP एक त्रुटि संदेश भेजने के लिए ICMP का उपयोग करता है, और संदेश परिवहन करने के लिए ICMP, IP का उपयोग करता है।

ICMP प्रोटोकॉल द्वारा परिभाषित कुछ त्रुटि संदेशों का संक्षिप्त विवरण निम्नलिखित हैः

स्रोत शमन करना: एक राउटर या होस्ट जिसका संचार बफर प्राप्त होता है, लगभग पूर्ण रूप से सामान्य रूप से इस संदेश को ट्रिगर करता है। एक स्रोत शमन संदेश भेजने वाले होस्ट को भेजा जाता है, प्राप्तकर्त्ता केवल भेजने वाले होस्ट से अनुरोध करता है कि वह उस दर को कम करे जिस पर वह अन्यथा सलाह देने तक संचारित हो रहा है।

समय बढ़ना: दो दशाओं में एक समय से अधिक संदेश भेजा गया है। जब भी कोई राउटर डेटा ग्राम में TIL फील्ड को शून्य पर कम करता है। राउटर डेटाग्राम को छोड़ देता है और एक समय से अधिक संदेश भेजता है।

इसके अतिरिक्त एक समय से अधिक हो चुके संदेश को एक होस्ट द्वारा भेजा जाता है यदि पुर्न–व्यवस्थित टाइमर किसी दिए गए आरेख से सभी टुकड़ों से पहले समाप्त हो जाता हो।

रूट रीडायरेक्ट: एक राउटर इस संदेश को एक होस्ट को भेजता है जो अपनी रूटिंग सेवाओं का अनुरोध कर रहा है। जब कोई होस्ट किसी नेटवर्क के लिए नियत किए गए डेटाग्राम को बनाता है, तो होस्ट डेटाग्राम को एक राउटर को भेजता है, जो डेटाग्राम को उसके गंतव्य तक भेज देता है। यदि एक राउटर यह निर्धारित करता है कि किसी होस्ट ने गलत तरीके से एक डेटाग्राम भेजा है जिसे एक अलग राउटर को भेजा जाना चाहिए, तो राउटर रूट रीडायरेक्ट संदेश का उपयोग करता है जिससे होस्ट को अपना रूट बदलने का कारण बनता है। इस विधि में, एक रूट रीडायरेक्ट संदेश रूटिंग प्रक्रिया की कार्यक्षमता को वांछित गंतव्य के लिए एक छोटे पथ के अनुरोध होस्ट को सूचित करके सुधारता है।

होस्ट अगम्य: जब भी कोई प्रवेश द्वार या एक राउटर निर्धारित करता है कि डेटाग्राम को अपने अंतिम गंतव्य (लिंक विफलता या बैंडविड्थ की भीड़ के कारण) तक नहीं पहुंचाया जा सकता है, तो एक ICMP होस्ट अप्राप्य संदेश नेटवर्क पर मूल नोड को भेजा जाता है। आम तौर पर, संदेश में वह कारण सम्मिलित होता है जिसके कारण होस्ट तक नहीं पहुँचा जा सकता है।

विखंडन और पुर्न–व्यवस्थित: वह वृहद डाटाग्राम जिसे IP प्रोटोकॉल संभाल सकता है 64 किलोबाइट का होता है। IP हेडर में कुल लंबाई फील्ड की चौड़ाई से अधिकतम डेटाग्राम आकार तय होता है।

वास्तविक रूप से, अधिकांश अंतर्निहित डेटा लिंक प्रौद्योगिकियाँ इस डेटा आकार को समायोजित नहीं कर सकती हैं। उदाहरण के लिए, ईथरनेट द्वारा समर्थित डेटा फ्रेम का अधिकतम आकार 1,514 बाइट्स है। जब तक इस तरह की स्थितियों के बारे में कुछ नहीं किया जाता है, IP को डेटा लिंक को छोड़ना पड़ता है जो इसे ऊपरी परत प्रोटोकॉल से वितरित किया जाता है, डेटा लिंक परत द्वारा अधिकतम सहनीय आकार से अधिक आकार के साथ। इस कठिनाई को दूर करने के लिए, IP को डेटा विखंडन और पुर्न–व्यवस्थित प्रदान करने के लिए बनाया गया है।

ICMP संदेश परिवहनः

ICMP प्रत्येक त्रुटि संदेश को ले जाने के लिए IP का उपयोग करता है। जब राउटर के पास भेजने के लिए एक ICMP संदेश होता है, तो यह डेटाग्राम बनाता है और डेटा में ICMP संदेश को एन्क्रिप्ट करता है। इसका अर्थ है कि IP डेटा ग्राम के डेटा क्षेत्र में रखा गया ICMP संदेश। डेटाग्राम को सदैव के समान पूरा डेटाग्राम ट्रांसमिशन के लिए एक फ्रेम में संपुटित किया जाता है।

ICMP, TCP/IP के अंदर एक परिवहन स्तर का प्रोटोकॉल है जो नेटवर्क कनेक्टिविटी की समस्याओं के बारे में सूचना को संचारित ट्रांसमिशन के स्रोत तक पहुँचाता है। यह नियंत्रण संदेश भेजता है जैसे गंतव्य नेटवर्क पहुँच योग्य, स्रोत मार्ग विफल, और स्रोत शमन। यह 8–बाइट हेडर और चर–आकार डेटा अनुभाग के साथ डेटा पैकेट संरचना का उपयोग करता है।

ट्रांसमिशन परिस्थतियों के बारे में डेटा पैकेट के स्रोत के साथ संवाद करने के लिए, ICMP का उपयोग राउटर जैसे उपकरण द्वारा किया जाता है। उदाहरण के लिए, यदि कोई डाटाग्राम डिलीवर नहीं किया जाता है, तो ICMP इसे वापस होस्ट को विवरण के साथ रिपोर्ट करने में मदद कर सकता है कि ट्रांसमिशन कहाँ गलत हुआ। यह एक प्रोटोकॉल है जो कार्यस्थल में सीधे संचार पर विश्वास करता है।

ध्वनि स्पंद एक उपयोगिता है जो नेटवर्क कनेक्टिविटी और एक होस्ट और एक गंतव्य कम्प्यूटर के मध्य डेटा रिले की गति की जानकारी वापस रिपोर्ट करने के लिए ICMP संदेशों का उपयोग करता है। यह उन कुछ उदाहरणों में से एक है जहाँ उपयोगकर्ता सीधे ICMP के साथ संवाद कर सकता है, जो आमतौर पर केवल नेटवर्क वाले कम्प्यूटर को एक दूसरे के साथ स्वचालित रूप से संवाद करने की अनुमति देने के लिए कार्य करता है।

8.3 नेटवर्क सुरक्षा के लक्ष्य:

जैसा कि पहले अनुच्छेदों में चर्चा की गई है, नेटवर्क में बड़ी संख्या में कमियाँ उपलब्ध हैं। इस प्रकार, संचरण के समय, डेटा हमलों के लिए अत्यधिक असुरक्षित है। एक हमलावर संचार चैनल को लक्षित कर सकता है, डेटा प्राप्त कर सकता है और अपने नापाक उद्देश्यों को प्राप्त करने के लिए एक ही संदेश पढ़ सकता है या एक गलत संदेश डाल सकता है।

नेटवर्क सुरक्षा न केवल संचार श्रृंखला के प्रत्येक छोर पर कम्प्यूटर की सुरक्षा के बारे में चिंतित है, बल्कि, यह सुनिश्चित करना है कि पूरा नेटवर्क सुरक्षित है। नेटवर्क सुरक्षा नेटवर्क और डेटा की उपयोगिता, विश्वसनीयता, अखंडता, और सुरक्षा की रक्षा करती है। प्रभावी नेटवर्क सुरक्षा एक नेटवर्क पर प्रवेश करने या फैलने से विभिन्न प्रकार के खतरों को हरा देती है।

नेटवर्क सुरक्षा का प्राथमिक लक्ष्य गोपनीयता, अखंडता और उपलब्धता है। नेटवर्क सुरक्षा के इन तीन स्तंभों को अक्सर CIA त्रिकोण के रूप में दर्शाया जाता है।

गोपनीयता: गोपनीयता का कार्य अनधिकृत व्यक्तियों से कीमती व्यापार डेटा की रक्षा करना है। नेटवर्क सुरक्षा का गोपनीयता भाग यह सुनिश्चित करता है कि डेटा केवल इच्छित और अधिकृत व्यक्तियों के लिए उपलब्ध है।

अखंडता: इस लक्ष्य का मतलब डेटा की सटीकता और स्थिरता को बनाए रखना और सुनिश्चित करना है। अखंडता का कार्य यह सुनिश्चित करना है कि डेटा विश्वसनीय है और अनधिकृत व्यक्तियों द्वारा परिवर्तित नहीं किया गया है।

उपलब्धता: नेटवर्क सुरक्षा में उपलब्धता का कार्य यह सुनिश्चित करना है कि डेटा, नेटवर्क संसाधन/सेवाएँ वैध उपयोगकर्ताओं के लिए लगातार उपलब्ध हों, जब भी उन्हें इसकी आवश्यकता हो।

हमें नेटवर्क सुरक्षा की आवश्यकता क्यों है?

नेटवर्क को हमलावरों और हैकर्स के खिलाफ सुरक्षा की आवश्यकता है। नेटवर्क सुरक्षा दो बुनियादी प्रतिभूतियों को सम्मिलित करती है। पहला डेटा जानकारी की सुरक्षा है अर्थात् जानकारी को अनधिकृत पहुँच और नुकसान से बचाने के लिए और दूसरा है कम्प्यूटर सुरक्षा अर्थात् डाटा की सुरक्षा और हैकर्स को नाकाम करना।

नेटवर्क सुरक्षा का उद्देश्य क्या है?

नेटवर्क सुरक्षा में अनधिकृत पहुँच, दुरुपयोग, संशोधन या कम्प्यूटर नेटवर्क–सुलभ संसाधनों से वंचित करने से रोकने और निगरानी करने के लिए अपनाई गई नीतियाँ और व्यवहार शामिल हैं।

नेटवर्क सुरक्षा के क्या लाभ हैं?

नेटवर्क सुरक्षा नेटवर्क पर मौजूद क्लाइंट के व्यक्तिगत डेटा को सुरक्षित रखने में मदद करती है। नेटवर्क सुरक्षा उन सूचनाओं के संरक्षण की सुविधा प्रदान करती है जो नेटवर्क पर कम्प्यूटर्स के मध्य साझा की जाती हैं। इंटरनेट से हैकिंग के प्रयास या वायरस/स्पाइवेयर हमले भौतिक कम्प्यूटर्स को नुकसान नहीं पहुँचा पाएंगे।

नेटवर्क सुरक्षा कैसे सहायक है?

नेटवर्क सुरक्षा प्रणाली का मुख्य उद्देश्य और भूमिका हमारे हार्डवेयर नेटवर्क को सुरक्षित करने की प्रक्रिया है जिसमें कई हार्डवेयर और सॉफ्टवेयर घटकों का उपयोग किया जाता है। आम तौर पर नेटवर्क सुरक्षा प्रणाली विश्वसनीयता, सुरक्षा, अखंडता और हमारे सिस्टम की उपयोगिता की रक्षा करती है जिससे नेटवर्क पर सुरक्षित तारीख सुनिश्चित होती है।

8.4 नेटवर्क सुरक्षा प्राप्त करना:

नेटवर्क सुरक्षा सुनिश्चित करना बहुत सरल प्रतीत हो सकता है। प्राप्त किए जाने वाले लक्ष्य सीधे–सादे प्रतीत होते हैं, लेकिन वास्तव में, इन लक्ष्यों को प्राप्त करने के लिए उपयोग किए जाने वाले तंत्र अत्यधिक जटिल हैं, और उन्हें समझने में ध्वनि तर्क शामिल है।

अंतर्राष्ट्रीय दूरसंचार संघ (ITU) ने सुरक्षा वास्तुकला X.800 पर अपनी सिफारिश में, नेटवर्क सुरक्षा प्राप्त करने के लिए तरीकों में मानकीकरण लाने के लिए कुछ तंत्रों को परिभाषित किया है। इनमें से कुछ तंत्र हैंः

एन–सिफरमेंट: यह तंत्र अनधिकृत व्यक्तियों के लिए डेटा को पढ़ने योग्य रूपों में परिवर्तित करके डेटा गोपनीयता सेवाएं प्रदान करता है। यह तंत्र गुप्त कुंजियों के साथ एन्क्रिप्शन–डिक्रिप्शन एल्गोरिथ्म का उपयोग करता है।

डिजिटल हस्ताक्षर: यह तंत्र इलेक्ट्रॉनिक डेटा में साधारण हस्ताक्षर के इलेक्ट्रॉनिक समकक्ष है। यह डेटा की प्रामाणिकता प्रदान करता है।

अभिगम नियंत्रण: इस तंत्र का उपयोग अभिगम नियंत्रण सेवाओं को प्रदान करने के लिए किया जाता है। ये तंत्र इकाई के उपयोग के अधिकारों को निर्धारित करने और लागू करने के लिए किसी इकाई की पहचान और प्रमाणीकरण का उपयोग कर सकते हैं।

नेटवर्क सुरक्षा प्राप्त करने के लिए विभिन्न सुरक्षा तंत्र विकसित और पहचान किए जाने के बाद, यह तय करना आवश्यक है कि उन्हें कहाँ लागू किया जाए। दोनों भौतिक रूप से (किस स्थान पर) और तार्किक रूप से (TCP/IP जैसी वास्तुकला की किस परत पर)।

नेटवर्किंग परतों पर सुरक्षा तंत्रः

कई सुरक्षा तंत्र इस तरह से विकसित किए गए हैं कि उन्हें OSI नेटवर्क परत मॉडल की एक विशिष्ट परत पर विकसित किया जा सकता है।

एप्लीकेशन परत पर सुरक्षा – इस परत पर उपयोग किए जाने वाले सुरक्षा उपाय अनुप्रयोग विशिष्टतः हैं। विभिन्न प्रकार के एप्लिकेशन को अलग–अलग सुरक्षा उपायों की आवश्यकता होगी। एप्लिकेशन परत सुरक्षा सुनिश्चित करने के लिए, अनुप्रयोगों को संशोधित करने की आवश्यकता है।

यह माना जाता है कि एक क्रिप्टोग्राफिक रूप से ध्वनि अनुप्रयोग प्रोटोकॉल को डिजाइन करना बहुत कठिन है और इसे ठीक से लागू करना और भी चुनौतीपूर्ण है।

इसलिए, नेटवर्क संचार की सुरक्षा के लिए एप्लीकेशन परत सुरक्षा तंत्र को केवल मानकों पर आधारित समाधान के रूप में पसंद किया जाता है जो कुछ समय के लिए उपयोग में रहा है।

एप्लीकेशन परत सिक्योरिटी प्रोटोकॉल का एक उदाहरण सिक्योर मल्टीपर्पज इंटरनेट मेल एक्सटेंशन्स (S/MIME) है, जिसका उपयोग आमतौर पर ई–मेल संदेशों को एन्क्रिप्ट करने के लिए किया जाता है। DNSSEC इस परत पर एक और प्रोटोकॉल है जिसका उपयोग DNS क्वेरी संदेशों के सुरक्षित आदान–प्रदान के लिए किया जाता है।

ट्रांसपोर्ट परत पर सुरक्षा – इस परत पर सुरक्षा उपायों का उपयोग दो होस्ट्स के मध्य एकल संचार सत्र में डेटा की सुरक्षा के लिए किया जा सकता है। ट्रांसपोर्ट परत सुरक्षा प्रोटोकॉल के लिए सबसे आम उपयोग HTTP और FTP सत्र ट्रैफिक की सुरक्षा है। ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) और सिक्योर सॉकेट लेयर (SSL) इस उद्देश्य के लिए उपयोग किए जाने वाले सबसे सामान्य प्रोटोकॉल हैं।

नेटवर्क परत – इस परत पर सुरक्षा उपायों को सभी अनुप्रयोगों पर लागू किया जा सकता है, इस प्रकार, वे अनुप्रयोग–विशिष्ट नहीं हैं। दो होस्ट्स या नेटवर्क के मध्य सभी नेटवर्क संचार को किसी भी एप्लीकेशन को संशोधित किए बिना इस स्तर पर संरक्षित किया जा सकता है। कुछ वातावरणों में, नेटवर्क परत सुरक्षा प्रोटोकॉल जैसे कि इंटरनेट प्रोटोकॉल सिक्योरिटी (IPsec) व्यक्तिगत अनुप्रयोगों पर नियंत्रण जोड़ने में कठिनाइयों के कारण ट्रांसपोर्ट या एप्लिकेशन परत नियंत्रण की तुलना में बहुत बेहतर समाधान प्रदान करता है। हालांकि, इस परत पर सुरक्षा प्रोटोकॉल कम संचार लचीलापन प्रदान करते हैं जो कुछ अनुप्रयोगों द्वारा आवश्यक हो सकते हैं।

संयोग से, एक उच्च स्तर पर काम करने के लिए डिजाइन किया गया एक सुरक्षा तंत्र निचली परतों पर डेटा के लिए सुरक्षा प्रदान नहीं कर सकता है, क्योंकि निचली परतें ऐसे कार्य करती हैं जिनके बारे में उच्चतर परतें अवगत नहीं हैं। इसलिए, नेटवर्क सुरक्षा को बढ़ाने के लिए कई सुरक्षा तंत्रों को तैनात करना आवश्यक हो सकता है।

नेटवर्क सुरक्षा – गंभीर आवश्यकताः

सूचना और कुशल संचार हर व्यवसाय की सफलता के लिए दो सबसे महत्वपूर्ण रणनीतिक मुद्दे हैं। संचार और भंडारण के इलेक्ट्रॉनिक साधनों के आगमन के साथ, अधिक से अधिक व्यवसायों को संचार, जानकारी संग्रहीत करने और संसाधनों को प्राप्त करने के लिए डेटा नेटवर्क का उपयोग करने के लिए स्थानांतरित कर दिया गया है। नेटवर्क इन्फ्रास्ट्रक्चर के विभिन्न प्रकार और स्तर हैं जो व्यवसाय चलाने के लिए उपयोग किए जाते हैं।

यह कहा जा सकता है कि आधुनिक दुनिया में नेटवर्क कम्प्यूटर की तुलना में व्यवसायों पर कुछ भी बड़ा प्रभाव नहीं पड़ा। लेकिन नेटवर्किंग अपने साथ सुरक्षा खतरों को लेकर आती है, जो यदि कम हो जाते हैं, तो नेटवर्किंग के लाभों को जोखिमों को कम करने की अनुमति देता है।

व्यापार में नेटवर्क की भूमिकाः

आजकल, कम्प्यूटर नेटवर्क को लगभग सभी व्यवसायों द्वारा एक संसाधन के रूप में देखा जाता है। यह संसाधन उन्हें उन सूचनाओं को एकत्र करने, विश्लेषण करने, व्यवस्थित करने और प्रसारित करने में सक्षम बनाता है जो उनके लाभ के लिए आवश्यक हैं। अधिकांश व्यवसायों ने प्रतिस्पर्धी बने रहने के लिए नेटवर्क स्थापित किए हैं।

कम्प्यूटर नेटवर्किंग की सबसे स्पष्ट भूमिका यह है कि संगठन केंद्रीय स्थान पर लगभग किसी भी प्रकार की जानकारी संग्रहीत कर सकते हैं और इसे नेटवर्क के माध्यम से वांछित स्थान पर प्राप्त कर सकते हैं।

नेटवर्क के लाभः

कम्प्यूटर नेटवर्किंग लोगों को सूचना और विचारों को आसानी से साझा करने में सक्षम बनाता है, इसलिए वे अधिक कुशलता और उत्पादकता से काम कर सकते हैं। नेटवर्क खरीद, बिक्री और ग्राहक सेवा जैसी गतिविधियों में सुधार करते हैं। नेटवर्किंग पारंपरिक व्यावसायिक प्रक्रियाओं को अधिक कुशल, अधिक प्रबंधनीय और कम खर्चीला बनाती है।

कम्प्यूटर नेटवर्क से व्यवसाय को आकर्षित करने वाले प्रमुख लाभ निम्न हैं:

संसाधन साझाकरण – एक व्यवसाय नेटवर्क से जुड़े घटकों और बाह्य उपकरणों को साझा करके हार्डवेयर पर खर्च की गई राशि को कम कर सकता है।

सुव्यवस्थित व्यावसायिक प्रक्रियाएँ – कम्प्यूटर नेटवर्क व्यवसायों को उनकी आंतरिक व्यावसायिक प्रक्रियाओं को सुव्यवस्थित करने में सक्षम बनाते हैं।

विभागों के मध्य सहयोग – जब व्यवसाय के दो या अधिक विभाग अपने नेटवर्क के चयनित भागों को जोड़ते हैं, तो वे व्यावसायिक प्रक्रियाओं को सुव्यवस्थित कर सकते हैं, जो सामान्य रूप से समय और प्रयास की मात्रा को बढ़ाते हैं और अक्सर उच्च उत्पादकता प्राप्त करने के लिए कठिनाइयों का सामना करते हैं।

बेहतर ग्राहक संबंध – नेटवर्क ग्राहकों को कई लाभ प्रदान करता है जैसे कि व्यापार करने में सुविधा, शीघ्र सेवा प्रतिक्रिया, आदि।

कई अन्य व्यवसाय विशिष्ट लाभ हैं जो नेटवर्किंग से प्राप्त होते हैं। इस तरह के लाभों ने सभी प्रकार के व्यवसायों के लिए कम्प्यूटर नेटवर्किंग को अपनाना आवश्यक बना दिया है।

8.5 नेटवर्क सुरक्षा की आवश्यकता:

कम्प्यूटर नेटवर्क की बढ़ती क्षमता के साथ आधुनिक तकनीक में प्रगति के कारण वायर्ड या वायरलेस नेटवर्क पर खतरे काफी बढ़ गए हैं। विभिन्न व्यापारिक लेनदेन के लिए आज की दुनिया में इंटरनेट के अत्यधिक उपयोग ने व्यावसायिक बौद्धिक संपदा पर सूचना की चोरी और अन्य हमलों की चुनौतियों का सामना किया है।

वर्तमान युग में, अधिकांश व्यवसाय नेटवर्क एप्लिकेशन के माध्यम से संचालित होते हैं, और इसलिए, सभी नेटवर्क पर हमला होने का खतरा होता है। व्यावसायिक नेटवर्क के लिए सबसे आम सुरक्षा डेटा अवरोधन और चोरी, और पहचान की चोरी हैं।

नेटवर्क सुरक्षा एक विशेष क्षेत्र है जो इस तरह के खतरों को विफल करने और एक व्यवसाय के कम्प्यूटर नेटवर्किंग बुनियादी ढांचे की उपयोगिता, विश्वसनीयता, अखंडता, और सुरक्षा प्रदान करने से संबंधित है।

व्यापार के लिए नेटवर्क सुरक्षा का महत्वः

व्यावसायिक आस्तियों की सुरक्षा – यह नेटवर्क सुरक्षा का प्राथमिक लक्ष्य है। एसेट्स का अर्थ है कम्प्यूटर नेटवर्क में संग्रहित जानकारी। सूचना कंपनी के किसी भी अन्य मूर्त संपत्ति के रूप में महत्वपूर्ण और मूल्यवान है। नेटवर्क सुरक्षा गोपनीय सूचना की अखंडता, सुरक्षा और सुरक्षित पहुँच से संबंधित है।

नियामक आवश्यकताओं का अनुपालन – नेटवर्क सुरक्षा उपायों से व्यवसायों को सूचना सुरक्षा के बारे में सरकार और उद्योग विशिष्ट नियमों के अनुपालन में मदद मिलती है।

सुरक्षित सहयोगात्मक कार्य – नेटवर्क सुरक्षा सह–कार्यकर्ता सहयोग को प्रोत्साहित करती है और ग्राहकों और आपूर्तिकर्ताओं के साथ संचार की सुविधा प्रदान करके उन्हें सुरक्षित नेटवर्क पहुँच प्रदान करती है। यह ग्राहक और उपभोक्ता के विश्वास को बढ़ाता है कि उनकी संवेदनशील जानकारी सुरक्षित है।

कम जोखिम – नेटवर्क सुरक्षा को अपनाने से सुरक्षा भंग के प्रभाव को कम किया जाता है, जिसमें कानूनी कार्रवाई शामिल है जो छोटे व्यवसायों को दिवालिया कर सकती है।

प्रतिस्पर्धात्मक लाभ प्राप्त करना – नेटवर्क के लिए एक प्रभावी सुरक्षा प्रणाली विकसित करना एक संगठन को एक प्रतिस्पर्धात्मक बढ़त देता है। इंटरनेट वित्तीय सेवाओं और ई–कॉमर्स के क्षेत्र में, नेटवर्क सुरक्षा प्रमुख महत्व रखती है।

नेटवर्क को हमलावरों और हैकर्स के विरूद्व सुरक्षा की आवश्यकता है। नेटवर्क सुरक्षा में दो बुनियादी प्रतिभूतियाँ सम्मिलित हैं। पहला डेटा जानकारी की सुरक्षा है अर्थात् जानकारी को अनधिकृत पहुँच और नुकसान से बचाने के लिए और दूसरा है कम्प्यूटर सुरक्षा अर्थात् डेटा की सुरक्षा और हैकर्स को नाकाम करना। यहाँ नेटवर्क सुरक्षा का अर्थ केवल किसी नेटवर्क या नेटवर्क के किसी एक नेटवर्क में सुरक्षा से नहीं है।

अब हमारी नेटवर्क सुरक्षा की आवश्यकता दो भागों में विभक्त हो गई है। एक सूचना सुरक्षा की आवश्यकता है और दूसरी कम्प्यूटर सुरक्षा की आवश्यकता है।

इंटरनेट या किसी संगठन के किसी भी नेटवर्क पर, हजारों महत्वपूर्ण सूचनाओं का प्रतिदिन आदान–प्रदान किया जाता है। हमलावरों द्वारा इस जानकारी का दुरुपयोग किया जा सकता है। निम्नलिखित कारणों से सूचना सुरक्षा की आवश्यकता हैः

1. इंटरनेट पर ही गुप्त सूचना उपयोगकर्ताओं की सुरक्षा के लिए। किसी अन्य व्यक्ति को इसे देखना या एक्सेस नहीं करना चाहिए।
2. अनधिकृत उपयोगकर्ताओं द्वारा आकस्मिक या जानबूझकर अवांछित संपादन से जानकारी की रक्षा करने के लिए।
3. सूचना को नुकसान से बचाने के लिए और उसे अपने गंतव्य तक सही तरीके से पहुँचाने के लिए।
4. विशिष्ट परिस्थितियों में प्रेषक द्वारा इनकार से बचाने के लिए किसी भी नोड द्वारा प्राप्त संदेश की पावती के लिए प्रबंधन करना।
5. एक उपयोगकर्ता को किसी दूसरे उपयोगकर्ता को तीसरे संदेश के नाम से कुछ संदेश भेजने के लिए प्रतिबंधित करना। उदाहरण के लिए, उपयोगकर्ता X अपनी स्वयं की रुचि के लिए एक संदेश बनाता है जिसमें कुछ अनुकूल निर्देश होते हैं और इसे उपयोगकर्ता Y को इस तरह भेजता है कि Y संगठन के प्रबंधक Z से आने वाले संदेश को स्वीकार करता है।
6. तात्कालिकता की दशा में संदेश को ट्रांसमिशन लाइनों/मार्ग में अवांछित देरी से बचाने के लिए, इसे समय पर आवश्यक गंतव्य तक पहुँचाने के लिए।
7. नेटवर्क में डेटा पैकेट या सूचना पैकेट को भटकने से बचाने के लिए असीम रूप से लंबे समय तक नेटवर्क में और इस तरह लाइन में बढ़ती भीड़ के कारण कुछ आंतरिक दोषों के कारण इसे पकड़ने में विफल रहता है।

नेटवर्क सुरक्षा के एक अन्य भाग में कम्प्यूटर सुरक्षा सम्मिलित है। कम्प्यूटर सुरक्षा का अर्थ नेटवर्क के कारण होने वाली अवांछित क्षति से हमारे कम्प्यूटर सिस्टम की रक्षा करना है। इस प्रकार की हानि का एक प्रमुख कारण वायरस और स्पाईवेयर हैं जो हमारी हार्ड डिस्क से सारी जानकारी मिटा सकते हैं या कभी–कभी वे पर्याप्त विनाशकारी भी हो सकते हैं और हार्डवेयर की समस्या भी पैदा कर सकते हैं।

निश्चित रूप से नेटवर्क को इस प्रकार के हानिकारक सॉफ्टवेयर से संरक्षित किया जाना चाहिए। जो लोग जानबूझकर इस प्रकार के सॉफ्टवेयर को नेटवर्क पर डालते हैं उन्हें हैकर्स कहा जाता है। चूंकि नेटवर्क कम्प्यूटर इसका भाग है, इसलिए हैकर्स से कम्प्यूटर सुरक्षा भी नेटवर्क सुरक्षा का एक भाग है। हैकर्स से कम्प्यूटर सुरक्षा की आवश्यकतायें निम्न प्रकार हैं:

- इसे संक्रमित फाइल्स से वायरस की प्रतिकृति और कैप्चर करने से संरक्षित किया जाना चाहिए।
- इसे वार्म्स और बमों से उचित सुरक्षा की जरूरत है।
- ट्रोजन हॉर्स से सुरक्षा की आवश्यकता है क्योंकि वे हमारे कम्प्यूटर के लिए पर्याप्त खतरनाक हैं।

अभ्यास

1. भौतिक नेटवर्क से क्या समझते हैं?
2. नेटवर्क प्रोटोकॉल (संदेशाचार) को समझाइए।
3. TCP/IP प्रोटोकॉल (संदेशाचार) क्या है?
4. DNS प्रोटोकॉल (संदेशाचार) पर टिप्पणी लिखिए।
5. ICMP प्रोटोकॉल (संदेशाचार) को समझाइए।
6. नेटवर्क सुरक्षा के कौन–कौन से लक्ष्य हैं?
7. नेटवर्क सुरक्षा कैसे प्राप्त कर सकते हैं?
8. नेटवर्क सुरक्षा की आवश्यकता क्यों है?

अध्याय – 9

एप्लीकेशन लेयर
(अनुप्रयोग परत)

क्लाइंट–सर्वर अनुप्रयोग के बाद भी विभिन्न व्यावसायिक सेवाएँ अब ऑनलाइन प्रदान की जाती हैं। सबसे लोकप्रिय रूप वेब अनुप्रयोग और ई–मेल हैं। दोनों अनुप्रयोगों में, क्लाइंट नामित सर्वर से संचार करता है और सेवाएं प्राप्त करता है।

किसी भी सर्वर अनुप्रयोग से सेवा का उपयोग करते समय, क्लाइंट और सर्वर अंतर्निहित इंट्रानेट या इंटरनेट पर बहुत सारी जानकारी का आदान–प्रदान करते हैं। हम इस तथ्य से अवगत हैं कि ये सूचना लेनदेन विभिन्न हमलों की चपेट में हैं।

नेटवर्क सुरक्षा हमलों के विरूद्व डेटा हासिल करने पर जोर देती है, जबकि यह एक नेटवर्क पर पारगमन में है। इस लक्ष्य को प्राप्त करने के लिए, कई वास्तविक समय के सुरक्षा प्रोटोकॉल तैयार किए गए हैं। इस तरह के प्रोटोकॉल को कम से कम निम्नलिखित प्राथमिक उद्देश्य प्रदान करने की आवश्यकता है:

- पक्ष एक दूसरे को प्रमाणित करने के लिए पारस्परिक रूप से बातचीत कर सकते हैं।
- नेटवर्क पर जानकारी का आदान–प्रदान करने से पहले एक गुप्त सत्र कुंजी स्थापित करें।
- एन्क्रिप्टेड रूप में जानकारी का आदान–प्रदान करें।

रोचक बात यह है कि ये प्रोटोकॉल नेटवर्किंग मॉडल की विभिन्न परतों पर काम करते हैं। उदाहरण के लिए, S/MIME प्रोटोकॉल एप्लिकेशन लेयर पर काम करता है, SSL प्रोटोकॉल ट्रांसपोर्ट लेयर पर काम करने के लिए विकसित किया जाता है, और IPsec प्रोटोकॉल नेटवर्क लेयर पर काम करता है।

यह OSI मॉडल की सबसे ऊपरी परत है। विभिन्न तरीकों से डेटा (सूचना) का हेरफेर इस परत में किया जाता है जो उपयोगकर्ता या सॉफ्टवेयर को नेटवर्क तक पहुँचने में सक्षम बनाता है। इस परत द्वारा प्रदान की जाने वाली कुछ सेवाओं में शामिल हैं: ई–मेल, फाइल्स स्थानांतरित करना, उपयोगकर्ता, निर्देशिका सेवाओं, नेटवर्क संसाधनों आदि के परिणाम वितरित करना।

एप्लिकेशन लेयर में विभिन्न प्रकार के प्रोटोकॉल होते हैं जिनकी आमतौर पर उपयोगकर्ताओं द्वारा आवश्यकता होती है। एक व्यापक रूप से इस्तेमाल किया जाने वाला अनुप्रयोग प्रोटोकॉल HTTP (Hyper Text Transfer Protocol) है, जो वर्ल्ड वाइड वेब का आधार है। जब कोई ब्राउजर वेब पेज चाहता है, तो वह उस पेज का नाम भेजता है जिसे वह HTTP का उपयोग कर सर्वर को चाहता है। सर्वर तब पेज को वापस भेजता है।

अन्य अनुप्रयोग प्रोटोकॉल जो उपयोग किए जाते हैं वे हैं: फाइल ट्रांसफर प्रोटोकॉल (FTP), ट्रिवियल फाइल ट्रांसफर प्रोटोकॉल (TFTP), सिंपल मेल ट्रांसफर प्रोटोकॉल (SMTP), TELNET, डोमेन नेम सिस्टम (DNS) आदि।

एक अनुप्रयोग परत या एप्लीकेशन लेयर एक अमूर्त परत है जो एक संचार नेटवर्क में होस्ट द्वारा उपयोग किए जाने वाले साझा संचार प्रोटोकॉल और इंटरफेस विधियों को निर्दिष्ट करती है। कम्प्यूटर नेटवर्किंग के मानक मॉडलः इंटरनेट प्रोटोकॉल सूट (TCP/IP) और OSI मॉडल दोनों में एप्लिकेशन लेयर पृथक्करण का उपयोग किया जाता है। यद्यपि दोनों मॉडल अपने संबंधित उच्चतम स्तर की परत के लिए एक ही शब्द का उपयोग करते हैं, विस्तृत परिभाषाएँ और उद्देश्य अलग–अलग हैं।

TCP/IP में, एप्लिकेशन परत में संचार प्रोटोकॉल और इंटरफेस विधियों का उपयोग इंटरनेट प्रोटोकॉल (IP) कम्प्यूटर नेटवर्क में प्रोसेस–टू–प्रोसेस संचार में किया जाता है। एप्लिकेशन परत केवल संचार को मानकीकृत करता है और होस्ट–से–होस्ट डेटा ट्रांसफर चैनल्स को स्थापित करने और क्लाइंट–सर्वर या पीयर–से–पीयर नेटवर्किंग मॉडल में डेटा एक्सचेंज का प्रबंधन करने के लिए अंतर्निहित ट्रांसपोर्ट लेयर प्रोटोकॉल पर निर्भर करता है। हालांकि TCP/IP एप्लिकेशन परत विशिष्ट नियमों या डेटा प्रारूपों का वर्णन नहीं करता है, जिन्हें संचार करते समय अनुप्रयोगों को विचार करना चाहिए, मूल विनिर्देश (आरएफसी 1123 में) निर्भर करता है और आवेदन डिजाइन के लिए मजबूती के सिद्धांत की सिफारिश करता है।

OSI मॉडल में, एप्लीकेशन परत की परिभाषा दायरे में संकीर्ण है। OSI मॉडल उपयोगकर्ता को प्राप्त जानकारी को प्रदर्शित करने के लिए जिम्मेदार उपयोगकर्त्ता इंटरफेस के रूप में एप्लिकेशन परत को परिभाषित करता है। इसके विपरीत, इंटरनेट प्रोटोकॉल सूट इस तरह के विवरण के साथ खुद को चिंतित नहीं करता है। OSI स्पष्ट रूप से एप्लिकेशन परत के नीचे अतिरिक्त कार्यक्षमता को अलग करता है, लेकिन परिवहन परत के ऊपर दो अतिरिक्त स्तरों परः सत्र परत, और प्रस्तुति परत। OSI इन परतों में कार्यक्षमता का एक सख्त मॉड्यूलर पृथक्करण निर्दिष्ट करता है और प्रत्येक परत के लिए प्रोटोकॉल कार्यान्वयन प्रदान करता है।

एप्लिकेशन परत में निम्नलिखित कार्य शामिल हैं:

- संचार साझेदारों की पहचानः एप्लिकेशन परत संचारित करने के लिए डेटा के साथ एक एप्लिकेशन के लिए संचार भागीदारों की उपलब्धता की पहचान करता है।
- संसाधन उपलब्धता का निर्धारणः आवेदन परत यह निर्धारित करता है कि अनुरोधित संचार के लिए पर्याप्त नेटवर्क संसाधन उपलब्ध हैं या नहीं।
- संचार को सिंक्रोनाइज करनाः अनुप्रयोगों के मध्य होने वाले सभी संचारों के लिए सहयोग की आवश्यकता होती है जो एक एप्लिकेशन परत द्वारा प्रबंधित की जाती है।

एप्लिकेशन परत की सेवाएं:

नेटवर्क वर्चुअल टर्मिनलः एक एप्लिकेशन परत उपयोगकर्ता को दूरस्थ होस्ट पर लॉग ऑन करने की अनुमति देता है। ऐसा करने के लिए, एप्लिकेशन दूरस्थ होस्ट पर एक टर्मिनल का एक सॉफ्टवेयर अनुकरण बनाता है। उपयोगकर्ता कम्प्यूटर सॉफ्टवेयर टर्मिनल से बात करता है, जो बदले में होस्ट से बात करता है। रिमोट होस्ट को लगता है कि यह अपने स्वयं के टर्मिनल्स में से एक के साथ संचार कर रहा है, इसलिए यह उपयोगकर्ता को लॉग ऑन करने की अनुमति देता है।

फाइल ट्रांसफर, एक्सेस और मैनेजमेंटः एक एप्लीकेशन एक उपयोगकर्ता को किसी दूरस्थ कम्प्यूटर में फाइल्स को एक्सेस करने, कम्प्यूटर से फाइल्स को पुनर्प्राप्त करने और एक दूरस्थ कम्प्यूटर में फाइल्स को प्रबंधित करने की अनुमति देता है। FTAM (File Transfer, Access and Management) फाइल संरचना, फाइल विशेषताओं और फाइल्स पर प्रदर्शन किए गए कार्यों और उनकी विशेषताओं के संदर्भ में एक पदानुक्रमित आभासी फाइल को परिभाषित करता है।

एड्रेसिंगः क्लाइंट और सर्वर के मध्य संचार प्राप्त करने के लिए, एड्रेसिंग की आवश्यकता होती है। जब एक क्लाइंट ने सर्वर से अनुरोध किया, तो अनुरोध में सर्वर का पता और अपना स्वयं का पता शामिल है। क्लाइंट अनुरोध के लिए सर्वर प्रतिक्रिया, अनुरोध में गंतव्य पता, अर्थात, क्लाइंट पता शामिल होता है। इस तरह के पते को प्राप्त करने के लिए, DNS का उपयोग किया जाता है।

मेल सेवाएँः एक आवेदन परत ईमेल अग्रेषण और भंडारण प्रदान करता है।

निर्देशिका सेवाएँः एक एप्लिकेशन में एक वितरित डेटाबेस होता है जो विभिन्न वस्तुओं और सेवाओं के बारे में वैश्विक जानकारी तक पहुँच प्रदान करता है।

प्रमाणीकरणः यह प्रेषक या रिसीवर के संदेश या दोनों को प्रमाणित करता है।

9.1 ई–मेल सुरक्षाः

आजकल, ई–मेल बहुत व्यापक रूप से उपयोग किया जाने वाला नेटवर्क अनुप्रयोग बन गया है। अब हम, सुरक्षा प्रोटोकॉल के बारे में जानने के लिए आगे बढ़ने से पहले ई–मेल के बुनियादी ढांचे पर चर्चा करेंगे।

ई–मेल की आधारिक संरचनाः

ई–मेल भेजने का सबसे सरल तरीका प्रेषक की मशीन से सीधे प्राप्तकर्ता की मशीन को संदेश भेजना होगा। इस दशा में, दोनों मशीनों के लिए नेटवर्क पर एक साथ चलना आवश्यक है। हालाँकि, यह व्यवस्था अव्यावहारिक है क्योंकि उपयोगकर्ता कभी–कभी अपनी मशीन्स को नेटवर्क से जोड़ सकते हैं।

इसलिए, ई–मेल सर्वर स्थापित करने की अवधारणा आ गई। इस व्यवस्था में, मेल एक मेल सर्वर को भेजा जाता है जो नेटवर्क पर स्थायी रूप से उपलब्ध होता है। जब प्राप्तकर्ता की मशीन नेटवर्क से जुड़ जाती है, तो वह मेल सर्वर से मेल पढ़ता है।

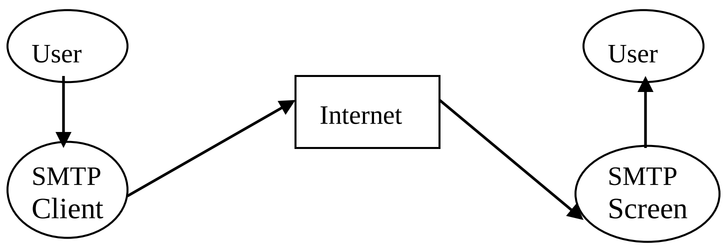
सामान्य तौर पर, ई–मेल आधारिक संरचना में मेल सर्वर्स का एक जाल होता है, जिसे मैसेज ट्रांसफर एजेंट्स (MTAs) और क्लाइंट मशीन भी कहा जाता है, जिसमें ई–मेल प्रोग्राम चलता है, जिसमें यूजर एजेंट (UA) और स्थानीय MTA शामिल होते हैं।

आमतौर पर, एक ई–मेल संदेश अपने UA से आगे हो जाता है, MTA के जाल से गुजरता है और अंत में प्राप्तकर्ता की मशीन पर UA तक पहुँचता है।

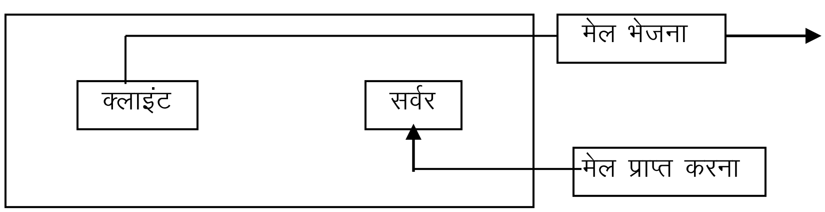
ई–मेल के लिए उपयोग किए जाने वाले प्रोटोकॉल निम्नानुसार हैं:

- ई–मेल संदेशों को अग्रेषित करने के लिए सरल मेल ट्रांसफर प्रोटोकॉल (SMTP) का उपयोग किया जाता है।
- पोस्ट ऑफिस प्रोटोकॉल (POP) और इंटरनेट मैसेज एक्सेस प्रोटोकॉल (IMAP) का उपयोग सर्वर से प्राप्तकर्ता द्वारा संदेश प्राप्त करने के लिए किया जाता है।

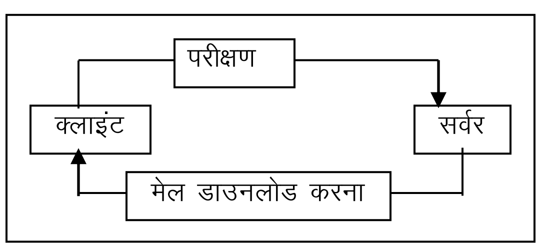
1. SMPT: इस प्रोटोकॉल की सहायता से ही ई–मेल एक कम्प्यूटर से दूसरे कम्प्यूटर तक पहुँचती है। यह TCP/IP परिवार का प्रोटोकॉल है। यह किसी मेल का एक सिस्टम से दूसरे सिस्टम तक पहुँचने का विवरण देता है।



2. POP: यह एक क्लाइंट सर्वर प्रोटोकॉल है। यह ई–मेल को डाउनलोड व अपलोड करने के काम आता है। POP की सहायता से प्रत्येक क्लाइंट सर्वर से अपने ई–मेल को प्राप्त करता है।



(SMTP)



(POP)

उपरोक्त दोनों प्रोटोकॉल के अतिरिक्त TCP/IP परिवार का प्रत्येक प्रोटोकॉल ई–मेल सर्वर में सहायता प्रदान करता है। जैसे – TCP, IP, UDP, UUCP, FTP, TELNET आदि।

MIME:

बेसिक इंटरनेट ई–मेल मानक 1982 में लिखा गया था और यह इंटरनेट पर एक्सचेंज किए गए ई–मेल संदेश के प्रारूप का वर्णन करता है। यह मुख्य रूप से मूल रोमन वर्णमाला में पाठ के रूप में लिखे गए ई–मेल संदेश का समर्थन करता है।

1992 तक, सुधार की आवश्यकता महसूस की जा रही थी। इसलिए, एक अतिरिक्त मानक बहुउद्देशीय इंटरनेट मेल एक्सटेंशन (MIME) परिभाषित किया गया था। यह बुनियादी इंटरनेट ई–मेल मानक के विस्तार का एक समूह है। MIME उन बुनियादी रोमन वर्णमाला जैसे कि सिरिलिक वर्णमाला (रूसी में प्रयुक्त), ग्रीक वर्णमाला, या यहाँ तक कि चीन के आईडियोग्राफिक वर्णमाला के अतिरिक्त अन्य वर्णमाला का उपयोग करके ई–मेल भेजने की क्षमता प्रदान करता है।

MIME द्वारा पूरी की गई एक और आवश्यकता अ–पाठ्य सामग्री, जैसे कि चित्र या वीडियो क्लिप भेजने की है। इन सुविधाओं के कारण, MIME मानक ई–मेल संचार के लिए SMTP के साथ व्यापक रूप से अपनाया गया।

ईमेल सुरक्षा, ईमेल संचार में संवेदनशील जानकारी रखने और अनधिकृत पहुँच, हानि या समझौता के विरूद्व सुरक्षित खातों के लिए विभिन्न तकनीकों का वर्णन करती है। ईमेल का उपयोग अक्सर मैलवेयर, स्पैम और फिशिंग हमलों को फैलाने के लिए किया जाता है। हमलावर संवेदनशील जानकारी के साथ भाग लेने के लिए भ्रामक संदेशों का उपयोग करते हैं, संलग्नक खोलते हैं या हाइपरलिंक पर क्लिक करते हैं जो पीड़ित के डिवाइस पर मैलवेयर स्थापित करते हैं। ईमेल भी एक एंटरप्राइज नेटवर्क में एक पैर जमाने और मूल्यवान कंपनी डेटा प्राप्त करने के लिए हमलावरों के लिए एक सामान्य प्रवेश बिंदु है।

ईमेल एन्क्रिप्शन में एन्क्रिप्टेड या भ्रामक, ईमेल संदेशों की सामग्री को संभावित प्राप्तकर्ता के अतिरिक्त किसी अन्य द्वारा पढ़ी जा रही संभावित संवेदनशील जानकारी से बचाने के लिए सम्मिलित है। ईमेल एन्क्रिप्शन में अक्सर प्रमाणीकरण सम्मिलित होता है।

ईमेल को संभव के रूप में खुला और सुलभ होने के लिए डिजाइन किया गया था। यह संगठनों में लोगों को एक दूसरे के साथ और अन्य संगठनों में लोगों के साथ संवाद करने की अनुमति देता है। समस्या यह है कि ईमेल सुरक्षित नहीं है। यह हमलावरों को लाभ के प्रयास में समस्या पैदा करने के तरीके के रूप में ईमेल का उपयोग करने की अनुमति देता है। चाहे स्पैम अभियानों, मैलवेयर और फिशिंग हमलों, परिष्कृत लक्षित हमलों, या व्यावसायिक ईमेल समझौता के माध्यम से, हमलावर अपने कार्यों को करने के लिए ईमेल की सुरक्षा की कमी का लाभ उठाने की कोशिश करते हैं। चूंकि अधिकांश संगठन व्यापार करने के लिए ईमेल पर भरोसा करते हैं, इसलिए संवेदनशील जानकारी चुराने की कोशिश में हमलावर ईमेल का फायदा उठाते हैं।

ईमेल सुरक्षा की आवश्यकताः

हमले के मार्ग के रूप में ईमेल की लोकप्रियता के कारण, यह महत्वपूर्ण है कि उद्यम और व्यक्ति अपने ईमेल खातों को आम हमलों के खिलाफ सुरक्षित करने के साथ–साथ खातों या संचार तक अनाधिकृत पहुँच के प्रयासों के लिए उपाय करते हैं।

ईमेल संदेशों के माध्यम से भेजे गए मैलवेयर काफी विनाशकारी हो सकते हैं। कर्मचारियों को भेजे गए फिशिंग ईमेल में अक्सर वैध दस्तावेजों की तरह दिखने के लिए डिजाइन किए गए अनुलग्नकों में मैलवेयर होते हैं या हाइपरलिंक्स सम्मिलित होते हैं जो मैलवेयर बनाने वाली वेबसाइट्स तक ले जाते हैं। एक ईमेल अटैचमेंट खोलना या ईमेल में एक लिंक पर क्लिक करना यह सब हो सकता है कि यह खातों या उपकरणों के लिए समझौता हो जाए।

फिशिंग ईमेल का उपयोग प्राप्तकर्ता को संवेदनशील जानकारी साझा करने के लिए किया जा सकता है, जिसे अक्सर एक वैध व्यवसाय या विश्वसनीय संपर्कों के रूप में प्रस्तुत किया जाता है। व्यवसायों के विरूद्व फिशिंग हमले अक्सर ऐसे विभागों को लक्षित करते हैं जो संवेदनशील व्यक्तिगत या वित्तीय जानकारी को संभालते हैं, जैसे कि देय खाते या मानव संसाधन। ज्ञात विक्रेताओं या कंपनी के अधिकारियों को प्रतिरूपण करने के अतिरिक्त, हमलावर अपनी सफलता की संभावनाओं को बढ़ाने के लिए फिशिंग ईमेल में तात्कालिकता की भावना पैदा करने की कोशिश करते हैं।

आम तौर पर जानकारी चुराने के उद्देश्य से फिशिंग ईमेल प्राप्तकर्ता को अपनी लॉगिन जानकारी, पासवर्ड, सामाजिक सुरक्षा नंबर, बैंक खाता संख्या और यहाँ तक कि क्रेडिट कार्ड की जानकारी की पुष्टि करने के लिए कहेंगे। कुछ नकली वेबसाइट्स से भी जुड़ते हैं, जो ठीक वैसा ही दिखता है जैसा पीड़ितों या कारोबारियों के भागीदार को खाता या वित्तीय जानकारी दर्ज करने के लिए धोखा देने के लिए।

ईमेल सुरक्षा उपकरणः

एक सुरक्षित ईमेल गेटवे, जिसे या तो ऑन–प्रिमाइसेस या क्लाउड में तैनात किया गया है, उसे अवांछित, दुर्भावनापूर्ण और BEC ईमेल से बहु–स्तरित सुरक्षा प्रदान करनी चाहिए, दानेदार दृश्यताय और सभी आकार के संगठनों के लिए व्यापार निरंतरता। ये नियंत्रण सुरक्षा टीमों को यह विश्वास दिलाने में सक्षम बनाते हैं कि वे उपयोगकर्ताओं को ईमेल के खतरों से सुरक्षित कर सकते हैं और आउटेज की स्थिति में ईमेल संचार बनाए रख सकते हैं।

एक ईमेल एन्क्रिप्शन समाधान आवश्यक व्यावसायिक संचार को सक्षम करते हुए नियामक उल्लंघन, डेटा हानि और कॉर्पोरेट नीति उल्लंघन से जुड़े जोखिमों को कम करता है। समाधान किसी भी संगठन के लिए काम करना चाहिए जो संवेदनशील डेटा की रक्षा करने की आवश्यकता है, जबकि अभी भी इसे संबद्धता, व्यापार भागीदारों और उपयोगकर्ताओं के लिए आसानी से उपलब्ध कर रहा है – डेस्कटॉप और मोबाइल डिवाइस दोनों पर। GDPR, HIPAA या SOX जैसे अनुपालन नियमों का पालन करने के लिए आवश्यक संगठनों के लिए एक ईमेल एन्क्रिप्शन समाधान विशेष रूप से महत्वपूर्ण है, या PCI&DSS जैसे सुरक्षा मानकों का पालन करता है।

9.2 ई–मेल सुरक्षा सेवायें:

महत्वपूर्ण लेनदेन के लिए ई–मेल संचार का बढ़ता उपयोग निम्नलिखित के रूप में कुछ मूलभूत सुरक्षा सेवाओं के प्रावधान की मांग करता हैः

गोपनीयता – ई–मेल संदेश किसी और के द्वारा नहीं पढ़ा जाना चाहिए केवल इच्छित प्राप्तकर्ता को छोड़कर।

प्रमाणीकरण – ई–मेल प्राप्तकर्ता प्रेषक की पहचान के बारे में सुनिश्चित हो सकता है।

वफादारी – प्राप्तकर्ता को आश्वासन है कि ई–मेल संदेश को प्रेषक द्वारा प्रेषित किए जाने के बाद बदल नहीं गया है।

गैर–अस्वीकरण – ई–मेल प्राप्तकर्ता तीसरे पक्ष को साबित करने में सक्षम है कि प्रेषक ने वास्तव में संदेश भेजा था।

प्रस्तुत करने का प्रमाण – ई–मेल भेजने वाले को यह पुष्टि मिलती है कि संदेश डाक वितरण प्रणाली को सौंप दिया गया है।

प्राप्ति का प्रमाण – प्रेषक को इस बात की पुष्टि हो जाती है कि प्राप्तकर्ता ने संदेश प्राप्त कर लिया है।

सार्वजनिक कुंजी क्रिप्टोग्राफी का उपयोग करके सुरक्षा सेवाएँ जैसे कि गोपनीयता, प्रमाणीकरण, संदेश अखंडता और गैर–अस्वीकृति प्रदान की जाती हैं।

आमतौर पर, ई–मेल संचार के तीन अलग–अलग परिदृश्य होते हैं। हम इन परिदृश्यों में उपरोक्त सुरक्षा सेवाओं को प्राप्त करने के तरीकों पर चर्चा करेंगे।

ईमेल सुरक्षा सेवाएँ प्रदाताः

ईमेल सुरक्षा सेवाओं को कंपनी के ईमेल खातों को अवांछनीय पहुँच और गलतफहमी से बचाने के लिए डिजाइन किया गया है, और कर्मचारी के ईमेल को हटाने, वायरस और चोरी से सुरक्षित किया गया है। ईमेल सुरक्षा प्रदाता रैंसमवेयर, फिशिंग, स्पूफिंग और अन्य ईमेल–संबंधी साइबर अपराध के वैश्विक मामलों को ट्रैक करने के लिए खतरे की खुफिया जानकारी का उपयोग करते हैं। प्रदाता इस जानकारी का उपयोग फायरवॉल और अन्य उपकरणों को डिजाइन करने और बनाए रखने के लिए करते हैं, जबकि कर्मचारियों को चीजों से बचने और अन्य सुरक्षा उपायों के लिए शिक्षित करते हैं। इन संयुक्त प्रयासों के माध्यम से, ईमेल सुरक्षा फर्म भ्रष्ट इनबाउंड संदेशों के संपर्क को कम करने और संवेदनशील आउटबाउंड संदेशों को सुरक्षित रखने में मदद करती हैं।

ईमेल सुरक्षा सेवाओं को डेटा सुरक्षा, अंतिम बिंदु सुरक्षा और अन्य साइबर सुरक्षा सेवाओं के साथ हाथों से जाना जाता है, ताकि कंपनियों को खतरों से अवगत कराया जा सके, हमलों से सुरक्षित रखा जा सके और किसी घटना की स्थिति में जवाब देने के लिए तैयार किया जा सके। व्यवसाय सुरक्षा प्रयासों को अधिकतम करने के लिए सुरक्षित ईमेल गेटवे और अन्य आईटी सुरक्षा सॉफ्टवेयर के बदले या ईमेल सुरक्षा सेवाओं के अतिरिक्त तैनात कर सकते हैं।

9.2.1 एक–से–एक ई–मेलः

इस परिदृश्य में, प्रेषक केवल एक प्राप्तकर्ता को एक ई–मेल संदेश भेजता है। आमतौर पर, दो से अधिक MTA संचार में सम्मिलित नहीं होते हैं। माना एक प्रेषक किसी प्राप्तकर्ता को एक गोपनीय ई–मेल भेजना चाहता है। इस मामले में गोपनीयता का प्रावधान इस प्रकार हैः

- प्रेषक और प्राप्तकर्त्ता के पास अपनी व्यक्तिगत–सार्वजनिक कुंजी क्रमशः (S_{PVT}, S_{PUB}) और (R_{PVT}, R_{PUB}) क्रमशः हैं।
- प्रेषक एन्क्रिप्शन के लिए एक गुप्त सममित कुंजी, K_S जनित करता है। यद्यपि प्रेषक एन्क्रिप्शन के लिए R_{PUB} का उपयोग कर सकता था, लेकिन तेजी से एन्क्रिप्शन और डिक्रिप्शन प्राप्त करने के लिए एक सममित कुंजी का उपयोग किया जाता है।
- प्रेषक कुंजी K_S के साथ संदेश एन्क्रिप्ट करता है और प्राप्तकर्ता के सार्वजनिक कुंजी R_{PUB} के साथ K_S को भी एन्क्रिप्ट करता है।
- प्रेषक प्राप्तकर्त्ता को एन्क्रिप्टेड संदेश और एन्क्रिप्टेड K_S भेजता है।
- प्राप्तकर्ता पहली बार K_S को अपनी व्यक्तिगत कुंजी, R_{PVT} का उपयोग करते हुए एनकोडेड K_S को डीक्रिप्ट करके प्राप्त करता है।
- प्राप्तकर्ता तब सममित कुंजी, K_S का उपयोग करके संदेश को डिक्रिप्ट करता है।

यदि इस परिदृश्य में संदेश अखंडता, प्रमाणीकरण और गैर–अस्वीकरण सेवाओं की भी आवश्यकता है, तो उपरोक्त प्रक्रिया में निम्नलिखित चरण जोड़े जाते हैं:

- प्रेषक संदेश का हैश जनित करता है और अपनी व्यक्तिगत कुंजी, S_{PVT} के साथ इस हैश को डिजिटल हस्ताक्षर करता है।
- प्रेषक इस हस्ताक्षरित हैश को अन्य घटकों के साथ प्राप्तकर्ता को भेजता है।
- प्राप्तकर्ता सार्वजनिक कुंजी S_{PUB} का उपयोग करता है और प्रेषक के हस्ताक्षर के तहत प्राप्त हैश निकालता है।
- प्राप्तकर्ता तब डिक्रिप्टेड संदेश को एन्क्रिप्ट करता है और अब दो हैश मानों की तुलना करता है। यदि वे मेल खाते हैं, तो संदेश अखंडता को प्राप्त करने के लिए माना जाता है।
- साथ ही, प्राप्तकर्ता सुनिश्चित है कि संदेश प्रेषक (प्रमाणीकरण) द्वारा भेजा गया है। और अंत में, प्रेषक इस बात से इनकार नहीं कर सकता है कि उसने संदेश (गैर–अस्वीकृति) नहीं भेजा था।

9.2.2 एक–से–बहुल प्राप्तकर्ता ई–मेलः

इस परिदृश्य में, प्रेषक दो या अधिक प्राप्तकर्ताओं को ई–मेल संदेश भेजता है। सूची को प्रेषक के ई–मेल प्रोग्राम (UA + local MTA) द्वारा प्रबंधित किया जाता है। सभी प्राप्तकर्ताओं को एक ही संदेश मिलता है।

माना, प्रेषक कई प्राप्तकर्ता (जैसे R1, R2 और R3) को गोपनीय ई–मेल भेजना चाहता है। इस दशा में गोपनीयता का प्रावधान निम्न प्रकार हैः

- प्रेषक और सभी प्राप्तकर्ताओं के पास व्यक्तिगत–सार्वजनिक कुंजी का अपना युग्म है।
- प्रेषक एक गुप्त सममित कुंजी बनाता है, K_s और इस कुंजी के साथ संदेश को एन्क्रिप्ट करता है।

- इसके बाद प्रेषक, $R1_{PUB}(K_S)$, $R2_{PUB}(K_S)$ और $R3_{PUB}(K_S)$ को प्राप्त करते हुए R1, R2 और R3 की सार्वजनिक कुंजियों के साथ K_S को कई बार एन्क्रिप्ट करता है।
- प्रेषक एन्क्रिप्टेड संदेश और एन्क्रिप्टेड K_S प्राप्तकर्ता भेजता है। उदाहरण के लिए, प्राप्तकर्ता (R1) एन्क्रिप्टेड संदेश और $R1_{PUB}(K_S)$ प्राप्त करता है।
- प्रत्येक प्राप्तकर्ता पहले अपनी व्यक्तिगत कुंजी का उपयोग करते हुए एनकोडेड K_S को डिक्रिप्ट करके कुंजी K_S निकालता है।
- प्रत्येक प्राप्तकर्ता तब सममित कुंजी, K_S का उपयोग करके संदेश को डिक्रिप्ट करता है।

संदेश की अखंडता, प्रमाणीकरण और गैर–अस्वीकृति प्रदान करने के लिए, इसके बाद किए जाने वाले चरण एक–से–एक ई–मेल परिदृश्य में ऊपर बताए गए चरणों के समान हैं।

9.2.3 एक–से–वितरण सूची ई–मेलः

इस परिदृश्य में, प्रेषक दो या अधिक प्राप्तकर्ताओं को एक ई–मेल संदेश भेजता है लेकिन प्राप्तकर्ता की सूची स्थानीय रूप से प्रेषक द्वारा प्रबंधित नहीं की जाती है। आम तौर पर, ई–मेल सर्वर मेलिंग सूची को बनाए रखता है।

प्रेषक मेल सूची को प्रबंधित करने के लिए MTA को एक मेल भेजता है और फिर सूची में सभी प्राप्तकर्ताओं को MTA द्वारा मेल किया जाता है।

इस दशा में, जब प्रेषक मेलिंग सूची के प्राप्तकर्ताओं को एक गोपनीय ई–मेल भेजना चाहता है (जैसे R1, R2 और R3), गोपनीयता इस प्रकार सुनिश्चित की गई हैः

- प्रेषक और सभी प्राप्तकर्ताओं के पास व्यक्तिगत–सार्वजनिक कुंजी का अपना युग्म है। एक्सप्लोडर सर्वर के पास प्रत्येक मेलिंग सूची ($List_{PUB}$, $List_{PVT}$) के लिए व्यक्तिगत–सार्वजनिक कुंजी का एक युग्म होता है।
- प्रेषक एक गुप्त सममित कुंजी K_s बनाता है और फिर इस कुंजी के साथ संदेश को एन्क्रिप्ट करता है।

तब प्रेषक K_S को सूची से संबद्ध सार्वजनिक कुंजी के साथ एन्क्रिप्ट करता है, $List_{PUB}(K_S)$ प्राप्त करता है।

प्रेषक एन्क्रिप्टेड संदेश और $List_{PUB}(K_S)$ भेजता है। एक्सप्लोडर MTA, $List_{PVT}$ का उपयोग करके $List_{PUB}(K_S)$ को डिक्रिप्ट करता है और K_S को प्राप्त करता है।

सूची में सदस्य के रूप में कई सार्वजनिक कुंजी के साथ एक्सप्लोडर K_S को एन्क्रिप्ट करता है। एक्सप्लोडर सूची के सभी प्राप्तकर्त्ता को प्राप्त एन्क्रिप्टेड संदेश और एन्क्रिप्ट किए गए संगत K_S को भेजता है। उदाहरण के लिए, एक्स्प्लोडर एन्क्रिप्टेड संदेश और $R1_{PUB}(K_S)$ को प्रथम प्राप्तकर्ता को भेजता है और इसी प्रकार।

संदेश की अखंडता, प्रमाणीकरण और गैर–अस्वीकृति प्रदान करने के लिए विभिन्न चरण एक–से–एक ई–मेल परिदृश्य की दशा में दिए गए चरणों के समान हैं।

रोचक बात यह है कि ई–मेल प्राप्त करने के लिए सुरक्षा पद्धति के ऊपर काम करने वाला ई–मेल प्रोग्राम उपरोक्त सभी संभावित परिदृश्यों के लिए काम करने की उम्मीद करता है। ई–मेल के लिए उपर्युक्त अधिकांश सुरक्षा तंत्र दो लोकप्रिय योजनाओं, प्रिटी गुड प्राइवेसी (Pretty Good Privacy - PGP) और S/MIME द्वारा प्रदान किए जाते हैं।

9.3 PGP

प्रिटी गुड प्राइवेसी (Pretty Good Privacy - PGP) एक ई–मेल एन्क्रिप्शन स्कीम है। यह ई–मेल संचार के लिए सुरक्षा सेवाएं प्रदान करने के लिए वास्तविक मानक बन गया है। जैसा कि पूर्व में चर्चा की गई है, यह सार्वजनिक कुंजी क्रिप्टोग्राफी, सममित कुंजी क्रिप्टोग्राफी, हैश फंक्शन और डिजिटल हस्ताक्षर का उपयोग करता है। यह निम्न सुविधा प्रदान करता हैः

- गोपनीयता
- प्रेषक प्रमाणीकरण
- संदेश की अखंडता
- अ–परित्याग

इन सुरक्षा सेवाओं के साथ, यह डेटा संपीड़न और प्रमुख प्रबंधन सहायता भी प्रदान करता है। PGP मौजूदा क्रिप्टोग्राफिक एल्गोरिथ्म जैसे RSA, IDEA, MD5 आदि का उपयोग करता है, न कि नए एल्गोरिथ्म का आविष्कार करके।

पीजीपी की कार्यप्रणालीः

- संदेश की हैश की गणना की जाती है। (MD5 एल्गोरिथ्म)
- परिणाम 128 बिट हैश को भेजने वाले (RSA एल्गोरिथ्म) की व्यक्तिगत कुंजी का उपयोग करके हस्ताक्षरित किया जाता है।
- डिजिटल हस्ताक्षर संदेश के लिए संक्षिप्त है, और परिणाम संकुचित है।
- एक 128–बिट सममित कुंजी, K_S जनित होता है और IDEA के साथ संपीड़ित संदेश को एन्क्रिप्ट करने के लिए उपयोग किया जाता है।
- K_S को RSA एल्गोरिथ्म का उपयोग करके प्राप्तकर्ता की सार्वजनिक कुंजी का उपयोग करके एन्क्रिप्ट किया जाता है और परिणाम एन्क्रिप्टेड संदेश से जुड़ा हुआ है।

IDs इंगित करती है कि किस कुंजी का उपयोग K_S को एन्क्रिप्ट करने के लिए किया जाता है और किस कुंजी का उपयोग हैश पर हस्ताक्षर को सत्यापित करने के लिए किया जाता है। PGP योजना में, हस्ताक्षरित और एन्क्रिप्ट किया गया संदेश, और फिर MIME प्रसारण से पहले एन्कोडेड है।

पीजीपी प्रमाण पत्रः

PGP कुंजी प्रमाणपत्र आम तौर पर विश्वास की एक श्रृंखला के माध्यम से स्थापित किया जाता है। उदाहरण के लिए, A की सार्वजनिक कुंजी को B अपनी सार्वजनिक कुंजी का उपयोग करके हस्ताक्षरित करता है और B की सार्वजनिक कुंजी को C अपनी सार्वजनिक कुंजी का उपयोग करके हस्ताक्षरित करता है। जैसे–जैसे यह प्रक्रिया आगे बढ़ती है, यह विश्वास की एक वेब स्थापित करता है।

PGP परिवेश में, कोई भी उपयोगकर्ता प्रमाणित प्राधिकारी के रूप में कार्य कर सकता है। कोई भी PGP उपयोगकर्ता किसी अन्य PGP उपयोगकर्ता की सार्वजनिक कुंजी प्रमाणित कर सकता है। हालांकि, इस तरह का एक प्रमाण पत्र केवल किसी अन्य उपयोगकर्ता के लिए मान्य होता है यदि उपयोगकर्ता प्रमाणक को विश्वसनीय परिचयकर्ता के रूप में पहचानता है।

इस प्रकार की प्रमाणन पद्धति के साथ कई मुद्दे उपलब्ध हैं। एक ज्ञात और विश्वसनीय सार्वजनिक कुंजी से वांछित कुंजी तक जाने वाली श्रृंखला को ढूंढना मुश्किल हो सकता है। इसके अतिरिक्त, कई श्रृंखलाएं हो सकती हैं जो वांछित उपयोगकर्ता के लिए अलग–अलग कुंजियों को जन्म दे सकती हैं। PGP प्रमाणीकरण प्राधिकारी के साथ PKI के बुनियादी ढांचे का उपयोग भी कर सकता है और सार्वजनिक कुंजी को CA (X.509 प्रमाण पत्र) द्वारा प्रमाणित किया जा सकता है।

PGP एक एन्क्रिप्शन प्रोग्राम है जो डेटा संचार के लिए क्रिप्टोग्राफिक गोपनीयता और प्रमाणीकरण प्रदान करता है। PGP का उपयोग हस्ताक्षर, एन्क्रिप्ट करने और डिक्रिप्ट करने के लिए टेक्स्ट, ई–मेल, फाइल्स, निर्देशिकाओं और संपूर्ण डिस्क विभाजन के लिए और ई–मेल संचार की सुरक्षा बढ़ाने के लिए किया जाता है। फिल जिमरमैन ने 1991 में पीजीपी विकसित किया। डेटा को एन्क्रिप्ट और डिक्रिप्ट करने के लिए PGP और इसी तरह के सॉफ्टवेयर OpenPGP मानक (RFC 4880) का अनुसरण करते हैं।

डिजाइनः

PGP एन्क्रिप्शन हैशिंग, डेटा संपीड़न, सममित–कुंजी क्रिप्टोग्राफी और अंततः सार्वजनिक–कुंजी क्रिप्टोग्राफी के एक क्रमिक संयोजन का उपयोग करता है। प्रत्येक चरण कई समर्थित एल्गोरिथ्म में से एक का उपयोग करता है। प्रत्येक सार्वजनिक कुंजी उपयोगकर्ता नाम या ई–मेल पते से जुड़ी होती है।

इस प्रणाली के पहले संस्करण को आम तौर पर X.509 प्रणाली के साथ विपरीत करने के लिए विश्वास की एक वेब के रूप में जाना जाता था, जो प्रमाण पत्र प्राधिकरण के आधार पर एक पदानुक्रमित दृष्टिकोण का उपयोग करता है और जिसे बाद में PGP कार्यान्वयन में जोड़ा गया था। PGP एन्क्रिप्शन के वर्तमान संस्करणों में एक स्वचालित कुंजी प्रबंधन सर्वर के माध्यम से दोनों विकल्प शामिल हैं।

PGP फिंगरप्रिंटः

सार्वजनिक कुंजी फिंगरप्रिंट एक सार्वजनिक कुंजी का एक छोटा संस्करण है। एक फिंगरप्रिंट से, किसी को सही संगत सार्वजनिक कुंजी मिल सकती है। C3A6 5E46 7B54 77DF 3C4C 9790 4D22 B3CA 5B32 FF66 जैसे फिंगरप्रिंट को बिजनेस कार्ड पर प्रिंट किया जा सकता है।

संगतताः

जैसे ही PGP विकसित होता है, नए फीचर और एल्गोरिथ्म का समर्थन करने वाले संस्करण एन्क्रिप्टेड संदेश बनाने में सक्षम होते हैं जो पुराने PGP सिस्टम को वैध निजी कुंजी के साथ भी डिक्रिप्ट नहीं कर सकते हैं। इसलिए, यह आवश्यक है कि PGP संचार में भागीदार एक–दूसरे की क्षमताओं को समझें या कम से कम PGP व्यवस्था पर सहमत हों।

गोपनीयताः

गोपनीय रूप से संदेश भेजने के लिए PGP का उपयोग किया जा सकता है। इसके लिए, PGP सममित–कुंजी एन्क्रिप्शन और सार्वजनिक–कुंजी एन्क्रिप्शन का संयोजन करके हाइब्रिड क्रिप्टोसिस्टम का उपयोग करता है। संदेश एक सममित एन्क्रिप्शन एल्गोरिथ्म का उपयोग करके एन्क्रिप्ट किया जाता है, जिसके लिए प्रेषक द्वारा उत्पन्न एक सममित कुंजी की आवश्यकता होती है। सममित कुंजी केवल एक बार उपयोग की जाती है और इसे सत्र कुंजी भी कहा जाता है। संदेश और उसकी सत्र कुंजी प्राप्तकर्त्ता को भेजी जाती है। सत्र कुंजी को प्राप्तकर्त्ता को भेजा जाना चाहिए ताकि वे संदेश को डिक्रिप्ट करना जानते हों, लेकिन ट्रांसमिशन के दौरान इसे सुरक्षित रखने के लिए इसे प्राप्तकर्त्ता की सार्वजनिक कुंजी के साथ एन्क्रिप्ट किया जाता है। केवल प्राप्तकर्त्ता से संबंधित व्यक्तिगत कुंजी सत्र कुंजी को डिक्रिप्ट कर सकती है, और संदेश को सममित रूप से डिक्रिप्ट करने के लिए इसका उपयोग कर सकती है।

डिजिटल हस्ताक्षरः

PGP संदेश प्रमाणीकरण और अखंडता जाँच का समर्थन करता है। बाद में इसका उपयोग यह पता लगाने के लिए किया जाता है कि क्या संदेश पूरा होने के बाद बदल दिया गया है।

साथ ही इसका उपयोग यह पूर्व निर्धारित करने के लिए किया जाता है कि क्या यह वास्तव में उस व्यक्ति या संस्था द्वारा भेजा गया था जिसने प्रेषक (एक डिजिटल हस्ताक्षर) होने का दावा किया था। क्योंकि सामग्री एन्क्रिप्ट की गई है, संदेश में कोई भी परिवर्तन उचित कुंजी के साथ डिक्रिप्शन की विफलता का परिणाम देगा। प्रेषक RSA या DSA एल्गोरिथ्म के साथ संदेश के लिए एक डिजिटल हस्ताक्षर बनाने के लिए PGP का उपयोग करता है। ऐसा करने के लिए, PGP प्लेन–टेक्स्ट से एक हैश (जिसे मैसेज डाइजेस्ट भी कहा जाता है) की गणना करता है और फिर प्रेषक की व्यक्तिगत कुंजी का उपयोग करके उस हैश से डिजिटल हस्ताक्षर बनाता है।

पीजीपी कैसे कार्य करता है?

PGP सार्वजनिक कुंजी प्रणाली की एक भिन्नता का उपयोग करता है। इस प्रणाली में, प्रत्येक उपयोगकर्ता के पास एक एन्क्रिप्शन कुंजी होती है जो सार्वजनिक रूप से जानी जाती है और एक व्यक्तिगत कुंजी जो केवल उसी उपयोगकर्ता के लिए जानी जाती है। हम किसी ऐसे संदेश को एन्क्रिप्ट करते हैं जिसे हम किसी अन्य व्यक्ति को भेजते हैं। जब वे इसे प्राप्त करते हैं, तो वे इसे अपनी व्यक्तिगत कुंजी का उपयोग करके डिक्रिप्ट करते हैं। चूंकि संपूर्ण संदेश को एन्क्रिप्ट करना समय लेने वाला हो सकता है, PGP संदेश को एन्क्रिप्ट करने के लिए तेज एन्क्रिप्शन एल्गोरिथ्म का उपयोग करता है और फिर सार्वजनिक कुंजी का उपयोग उस छोटी कुंजी को एन्क्रिप्ट करने के लिए करता है जिसका उपयोग संपूर्ण संदेश को एन्क्रिप्ट करने के लिए किया गया था। एन्क्रिप्ट किए गए संदेश और छोटी कुंजी दोनों को प्राप्तकर्त्ता को भेजा जाता है जो पहले छोटी कुंजी को डिक्रिप्ट करने के लिए प्राप्तकर्त्ता की व्यक्तिगत कुंजी का उपयोग करता है और फिर संदेश को डिक्रिप्ट करने के लिए उस कुंजी का उपयोग करता है।

पीजीपी दो सार्वजनिक कुंजी संस्करणों में आता है – रिवेस्ट–शमीर–एडलमैन (RSA) और डिफी–हेलमैन। RSA संस्करण, जिसके लिए PGP को RSA को लाइसेंस शुल्क का भुगतान करना होगा, लघु संदेश को एन्क्रिप्ट करने के लिए पूरे संदेश और RSA के लिए एक छोटी कुंजी उत्पन्न करने के लिए IDEA एल्गोरिथ्म का उपयोग करता है। डिफि–हेलमैन संस्करण संदेश को एन्क्रिप्ट करने के लिए लघु कुंजी हेतु CAST एल्गोरिथ्म का उपयोग करता है और लघु कुंजी को एन्क्रिप्ट करने के लिए डिफी–हेलमैन एल्गोरिथ्म का।

डिजिटल हस्ताक्षर भेजते समय, PGP एक कुशल एल्गोरिथ्म का उपयोग करता है जो उपयोगकर्ता के नाम और अन्य हस्ताक्षर जानकारी से एक हैश (एक गणितीय सारांश) उत्पन्न करता है। यह हैश कोड फिर प्रेषक की व्यक्तिगत कुंजी के साथ एन्क्रिप्ट किया गया है। प्राप्तकर्त्ता हैश कोड को डिक्रिप्ट करने के लिए प्रेषक की सार्वजनिक कुंजी का उपयोग करता है। यदि यह संदेश के लिए डिजिटल हस्ताक्षर के रूप में भेजे गए हैश कोड से सुमेलित होता है, तो प्राप्तकर्त्ता सुनिश्चित है कि संदेश कथित प्रेषक से सुरक्षित रूप से आ गया है। PGP का RSA संस्करण हैश कोड उत्पन्न करने के लिए MD5 एल्गोरिथ्म का उपयोग करता है। PGP का डिफी–हेलमैन संस्करण हैश कोड उत्पन्न करने के लिए SHA-1 एल्गोरिथ्म का उपयोग करता है।

पीजीपी प्राप्त करनाः

PGP का उपयोग करने के लिए, इसे डाउनलोड करें या क्रय कर अपने कम्प्यूटर सिस्टम पर स्थापित करें। इसमें आमतौर पर एक उपयोगकर्ता इंटरफेस होता है जो हमारे प्रथागत ईमेल प्रोग्राम के साथ काम करता है। हमें सार्वजनिक कुंजी को पंजीकृत करने की भी आवश्यकता हो सकती है जो हमारा PGP प्रोग्राम हमें PGP सार्वजनिक–कुंजी सर्वर के साथ देता है जिससे कि हम जिन लोगों के साथ संदेशों का आदान–प्रदान करते हैं वे हमारी सार्वजनिक कुंजी पा सकेंगे।

PGP फ्रीवेयर विंडोज, मैक, डॉस, यूनिक्स और अन्य ऑपरेटिंग सिस्टम के पुराने संस्करणों के लिए उपलब्ध है। 2010 में, सिमेंटेक कॉर्प ने PGP कॉर्प का अधिग्रहण किया, जिसने PGP कोड के अधिकार रखे और जल्द ही प्रौद्योगिकी के फ्रीवेयर संस्करण की पेशकश बंद कर दी।

विक्रेता वर्तमान में अपने विभिन्न एन्क्रिप्शन उत्पादों जैसे कि सिमेंटेक (Symantec) एन्क्रिप्शन डेस्कटॉप, सिमेंटेक डेस्कटॉप ईमेल एन्क्रिप्शन और सिमेंटेक एन्क्रिप्शन डेस्कटॉप संग्रहण जैसे PGP तकनीक प्रदान करता है। सिमेंटेक सहकर्मी समीक्षा के लिए सिमेंटेक एन्क्रिप्शन डेस्कटॉप स्रोत कोड भी उपलब्ध कराता है।

हालांकि सिमेंटेक ने PGP फ्रीवेयर को समाप्त कर दिया है, लेकिन प्रौद्योगिकी के अन्य गैर–मालिकाना संस्करण हैं जो उपलब्ध हैं। OpenPGP, PGP का एक खुला स्रोत संस्करण है जो इंटरनेट इंजीनियरिंग टास्क फोर्स (Internet Engineering Task Force - IETF) द्वारा समर्थित है। OpenPGP का उपयोग कई सॉफ्टवेयर विक्रेताओं द्वारा किया जाता है, जिसमें Coviant Software भी शामिल है, जो OpenPGP एन्क्रिप्शन के लिए एक निःशुल्क उपकरण और HushMail प्रदान करता है, जो OpenPGP द्वारा संचालित एक वेब–आधारित एन्क्रिप्टेड ईमेल सेवा प्रदान करता है। इसके अतिरिक्त, फ्री सॉफ्टवेयर फाउंडेशन ने एक OpenPGP अनुरूप एन्क्रिप्शन सॉफ्टवेयर जीएनयू प्राइवेसी गार्ड (GNU Privacy Guard - GPG) विकसित किया।

PGP का उपयोग कहाँ किया जाता हैं?

PGP का उपयोग डिजिटल सर्टिफिकेट और एन्क्रिप्ट/डिक्रिप्ट टेक्स्ट, ईमेल, फाइल, डायरेक्टरी और पूरे डिस्क पार्टीशन को एनक्रिप्ट करने के लिए किया जा सकता है। उदाहरण के लिए, सिमेंटेक, PGP आधारित उत्पादों जैसे कि सिमेंटेक फाइल साझा एन्क्रिप्शन के लिए एक नेटवर्क पर साझा की गई फाइलों को एन्क्रिप्ट करने के लिए और डेस्कटॉप, मोबाइल उपकरणों और हटाने योग्य भंडारण पर पूर्ण डिस्क एन्क्रिप्शन के लिए सिमेंटेक समापन बिंदु एन्क्रिप्शन प्रदान करता है। संदेशों के स्थान पर फाइल्स और ड्राइव्स के लिए PGP तकनीक का उपयोग करने की दशा में, सिमेंटेक उत्पाद उपयोगकर्ताओं को एकल साइन–ऑन के माध्यम से डेटा को डिक्रिप्ट और पुनः एन्क्रिप्ट करने की अनुमति देता है।

PGP एन्क्रिप्शन की कमियाँः

प्रशासन कठिन होता हैः PGP के विभिन्न संस्करण प्रशासन को जटिल बनाते हैं।

अनुकूलता मुद्देः प्रेषक और उपयोगकर्त्ता दोनों के पास PGP के संगत संस्करण होने चाहिए। उदाहरण के लिए, यदि हम किसी एन्क्रिप्शन तकनीक के साथ PGP का उपयोग करके किसी ईमेल को एन्क्रिप्ट करते हैं, तो यदि प्राप्तकर्त्ता के पास PGP का एक अलग संस्करण हो, तो वह डेटा को नहीं पढ़ सकेगा।

जटिलताः PGP एक जटिल तकनीक है। अन्य सुरक्षा योजनाएं सममित एन्क्रिप्शन का उपयोग करती हैं जो एक कुंजी या असममित एन्क्रिप्शन का उपयोग करता है, जो दो अलग–अलग कुंजी का उपयोग करता है। PGP एक हाइब्रिड दृष्टिकोण का उपयोग करता है जो दो कुंजी के साथ सममित एन्क्रिप्शन को लागू करता है। PGP अधिक जटिल है, और यह पारंपरिक सममित या असममित तरीकों से कम परिचित है।

वापस प्राप्ति नहींः कम्प्यूटर प्रशासक अपने पासवर्ड खोने की समस्याओं का सामना करते हैं। ऐसी स्थितियों में, एक व्यवस्थापक को पासवर्ड पुनः प्राप्त करने के लिए एक विशेष प्रोग्राम का उपयोग करना चाहिए। उदाहरण के लिए, एक तकनीशियन के पास एक कम्प्यूटर तक भौतिक पहुँच होती है, जिसका उपयोग पासवर्ड प्राप्त करने के लिए किया जा सकता है। हालांकि, PGP वसूली के लिए इस तरह के विशेष कार्यक्रम की पेशकश नहीं करता है। एन्क्रिप्शन के तरीके बहुत मजबूत हैं, इसलिए यह खोए हुए संदेशों या खो गई फाइल्स में पासवर्ड के परिणाम को पुनः प्राप्त नहीं करता है।

9.4 S/MIME:

S/MIME का अर्थ है सुरक्षित बहुउद्देशीय इंटरनेट मेल एक्सटेंशन (Secure Multipurpose Internet Mail Extension)। S/MIME एक सुरक्षित ई–मेल मानक है। यह MIME नामक पहले के असुरक्षित ई–मेलिंग मानक पर आधारित है।

S/MIME की कार्यप्रणालीः

S/MIME दृष्टिकोण PGP के समान है। यह सार्वजनिक कुंजी क्रिप्टोग्राफी, सममित कुंजी क्रिप्टोग्राफी, हैश फंक्शंस और डिजिटल हस्ताक्षर का भी उपयोग करता है। यह ई–मेल संचार के लिए PGP के समान सुरक्षा सेवाएं प्रदान करता है।

S/MIME में उपयोग किए जाने वाले सबसे सार्व सममित सिफर RC2 और ट्रिपल DES हैं। सामान्य सार्वजनिक कुंजी विधि RSA है, और हैशिंग एल्गोरिथ्म SHA-1 या MD5 है।

S/MIME एन्क्रिप्ट के उपरान्त डेटा आवरण के लिए अतिरिक्त MIME प्रकार को निर्दिष्ट करता है, जैसे application/pkcs7-mime। पूरे MIME इकाई को एन्क्रिप्ट किया गया है और एक ऑब्जेक्ट में रखा गया है। S/MIME ने क्रिप्टोग्राफिक संदेश प्रारूप (PGP से भिन्न) को मानकीकृत किया है। वास्तव में, MIME को कुछ कीवर्ड के साथ बढ़ाया जाता है ताकि संदेश में एन्क्रिप्टेड और/या हस्ताक्षरित भागों की पहचान की जा सके।

सार्वजनिक कुंजी वितरण के लिए S/MIME, X.509 प्रमाणपत्रों पर निर्भर करता है। प्रमाणन सहायता के लिए इसे शीर्ष–डाउन श्रेणीबद्ध PKI की आवश्यकता है।

S/MIME की रोजगारक्षमताः

कार्यान्वयन के लिए प्रमाणन प्राधिकरण से प्रमाण पत्र की आवश्यकता के कारण, सभी उपयोगकर्ता S/MIME का लाभ नहीं उठा सकते हैं, क्योंकि कुछ सार्वजनिक/व्यक्तिगत कुंजी जोड़ी के साथ एक संदेश को एन्क्रिप्ट करने की इच्छा कर सकते हैं। उदाहरण के लिए, प्रमाण पत्र की भागीदारी या प्रशासनिक उपरि के बिना।

व्यवहार में, हालांकि अधिकांश ई–मेलिंग एप्लिकेशन S/MIME को लागू करते हैं, प्रमाणपत्र नामांकन प्रक्रिया जटिल है। इसके स्थान पर PGP समर्थन को आमतौर पर प्लग–इन जोड़ने की आवश्यकता होती है और प्लग–इन उन सभी के साथ आता है जो कुंजी को प्रबंधित करने के लिए आवश्यक होते हैं। विश्वास का वेब वास्तव में उपयोग नहीं किया जाता है।

व्यक्ति अपनी सार्वजनिक कुंजियों का आदान–प्रदान दूसरे माध्यम से करते हैं। एक बार प्राप्त करने के बाद, वे उन लोगों की सार्वजनिक कुंजी की एक प्रति रखते हैं जिनके साथ आमतौर पर ई–मेल का आदान–प्रदान होता है।

PGP और S/MIME योजनाओं के लिए नेटवर्क आर्किटेक्चर में कार्यान्वयन परत में रहते हैं। ये दोनों योजनाएं ई–मेल संचार के लिए एप्लीकेशन परत की सुरक्षा प्रदान करती हैं।

योजनाओं में से एक, PGP या S/MIME, पर्यावरण के आधार पर उपयोग की जाती है। कैप्टिव नेटवर्क में एक सुरक्षित ई–मेल संचार PGP के लिए अनुकूल बनाकर प्रदान किया जा सकता है। इंटरनेट पर ई–मेल सुरक्षा के लिए, जहाँ मेलों का नए अज्ञात उपयोगकर्ताओं के साथ बहुत बार आदान–प्रदान किया जाता है, S/MIME को एक अच्छा विकल्प माना जाता है।

S/MIME कैसे कार्य करता है?

S/MIME ईमेल संदेशों को एन्क्रिप्ट करने, हस्ताक्षर करने और डिक्रिप्ट करने के लिए प्रमाणपत्रों के उपयोग की आवश्यकता होती है। प्रमाणपत्र केवल एक विशिष्ट प्रारूप में लिपटे हुए सार्वजनिक और/या व्यक्तिगत कुंजी हैं, ताकि उन्हें एक साथ उपयोग किया जा सके और विभिन्न प्रोग्राम्स द्वारा समझा जा सके। ईमेल आर्किटेक्चर उपकरण S/MIME ईमेल बनाने और प्राप्त करने के लिए उपयोग किए जा सकने वाले विभिन्न प्रमाणपत्रों को समाहित करने और प्रबंधित करने के लिए माइक्रोसॉफ्ट विंडोज प्रमाणपत्र भंडार पर निर्भर करते हैं।

एक S/MIME ईमेल संदेश पर हस्ताक्षर किए जा सकते हैं, एन्क्रिप्ट किया जा सकता है, या दोनों। संदेश के प्राप्तकर्ता के सार्वजनिक कुंजी प्रमाण पत्र का उपयोग करके संदेश को एन्क्रिप्ट किया जाता है। यह सुनिश्चित करता है कि केवल प्राप्तकर्ता संदेश को डिक्रिप्ट कर सकता है, क्योंकि एन्क्रिप्शन ऐसे किया जाता है ताकि केवल प्राप्तकर्ता की व्यक्तिगत कुंजी प्रमाणपत्र एन्क्रिप्शन को उलट सके। संदेश को प्रेषक की व्यक्तिगत कुंजी प्रमाण पत्र के साथ हस्ताक्षरित किया जाता है, और प्राप्तकर्ता को यह सुनिश्चित करता है कि संदेश भेजने वाला वह है जो वे कहते हैं कि वे हैं। संदेश की एक हैश भी हस्ताक्षर प्रक्रिया द्वारा बनाई गई है ताकि संदेश प्राप्त करने वाले को पता चले कि संदेश को लिखा जाने के बाद से नहीं बदला गया है।

जैसा कि PGP एन्क्रिप्शन/डिक्रिप्शन के साथ, कुंजी विनिमय की कुछ मात्रा की आवश्यकता होती है। किसी प्राप्तकर्ता को दिए गए संदेश एन्क्रिप्ट करने के लिए, प्रेषक के पास प्राप्तकर्ता के सार्वजनिक कुंजी प्रमाणपत्र की एक प्रति होनी चाहिए। यह आमतौर पर प्राप्तकर्ता द्वारा हस्ताक्षरित S/MIME ईमेल संदेश भेजने के द्वारा पूरा किया जाता है। S/MIME हस्ताक्षर इस प्रकार से किए जाते हैं कि प्रेषक का सार्वजनिक कुंजी प्रमाणपत्र बाद में उपयोग के लिए निकाला और संग्रहीत किया जा सकता है। माइक्रोसॉफ्ट आउटलुक एक्सप्रेस और मोजिला ईमेल क्लाइंट सहित अधिकांश आधुनिक ईमेल क्लाइंट स्वचालित रूप से एक हस्ताक्षरित संदेश को पहचान लेंगे, सार्वजनिक कुंजी प्रमाणपत्र निकालेंगे, और इसका परीक्षण करेंगे और बाद में उपयोग करने के लिए संग्राहीत करेंगे।

S/MIME प्रमाणपत्रः

किसी भी व्यक्ति को इन–हाउस प्रमाणपत्र प्राधिकारी (CA) से या सार्वजनिक CA से व्यक्तिगत कुंजी/प्रमाण पत्र प्राप्त करना चाहिए। सबसे अच्छा अभ्यास हस्ताक्षर के लिए और एन्क्रिप्शन के लिए पृथक–पृथक व्यक्तिगत कुंजी (और संबद्ध प्रमाण पत्र) का उपयोग करना है, क्योंकि यह हस्ताक्षर कुंजी की अ–संप्रेषण गुण से समझौता किए बिना एन्क्रिप्शन कुंजी के एस्क्रो को अनुमति देता है।

एन्क्रिप्शन को भंडार में गंतव्य पक्ष का प्रमाण पत्र रखने की आवश्यकता होती है (जो आमतौर पर एक वैध हस्ताक्षर प्रमाण पत्र के साथ पक्षकार से एक संदेश प्राप्त करने पर स्वचालित होता है)। जबकि तकनीकी रूप से यह संभव है कि किसी व्यक्ति को डिजिटल हस्ताक्षर करने के लिए बिना किसी प्रमाणपत्र (गंतव्य पक्ष का प्रमाण पत्र का उपयोग करना) के संदेश भेजना संभव है, व्यवहार में, S/MIME क्लाइंट को दूसरों को एन्क्रिप्ट करने की अनुमति देने से पहले उपयोगकर्ता को अपना प्रमाणपत्र स्थापित करने की आवश्यकता होगी।

एक विशिष्ट मूल ("class 1") व्यक्तिगत प्रमाण पत्र केवल मालिक की पहचान की पुष्टि करता है, क्योंकि यह घोषणा करता है कि प्रेषक 'From:' ईमेल पते का मालिक है इस अर्थ में कि प्रेषक उस पते पर भेजे गए ईमेल को प्राप्त कर सकता है, और इसलिए केवल यह सिद्व होता है कि प्राप्त एक ईमेल वास्तव में 'From:' पते से आया है। यह व्यक्ति के नाम या व्यवसाय के नाम को सत्यापित नहीं करता है। यदि कोई प्रेषक ईमेल प्राप्तकर्ताओं को प्रेषक की पहचान को सत्यापित करने के लिए इस अर्थ में सक्षम करना चाहता है कि प्राप्त प्रमाणपत्र नाम प्रेषक का नाम या किसी संगठन का नाम रखता है, तो प्रेषक को CA से प्रमाणपत्र ("class 2") प्राप्त करने की आवश्यकता होती है, अधिक गहराई से पहचान सत्यापन की प्रक्रिया, और इसमें प्रमाण–पत्र धारक के बारे में पूछताछ करना सम्मिलित है।

CA की नीति के आधार पर, प्रमाणपत्र और उसकी सभी सामग्री सार्वजनिक रूप से संदर्भ और सत्यापन के लिए पोस्ट की जा सकती है। यह नाम और ईमेल पता सभी को देखने और संभवतः खोजने के लिए उपलब्ध कराता है। अन्य CA केवल सरल क्रमांक और निरसन की स्थिति भेजते हैं, जिसमें व्यक्तिगत जानकारी सम्मिलित नहीं है। बाद में, कम से कम सार्वजनिक कुंजी बुनियादी ढांचे की अखंडता को बनाए रखने के लिए अनिवार्य है।

9.5 DNS सुरक्षा:

पूर्व में, हमने उल्लेख किया है कि एक हमलावर लक्ष्य उपयोगकर्ता पर हमले के लिए DNS कैश पॉइजनिंग का उपयोग कर सकता है। डोमेन नाम सिस्टम सुरक्षा एक्सटेंशन (Domain Name System Security Extensions - DNSSEC) एक इंटरनेट मानक है जो ऐसे हमलों को नाकाम कर सकता है।

एक मानक DNS योजना में, जब भी उपयोगकर्ता किसी डोमेन नाम से जुड़ना चाहता है, तो उसका कम्प्यूटर DNS सर्वर से संपर्क करता है और उस डोमेन नाम के लिए संबद्ध IP पते को देखता है। एक बार IP पता प्राप्त हो जाने के बाद, कम्प्यूटर उस IP पते से जुड़ जाता है।

इस योजना में, कोई सत्यापन प्रक्रिया सम्मिलित नहीं है। एक कम्प्यूटर एक वेबसाइट से जुड़े पते के लिए अपने DNS सर्वर से पूछता है, DNS सर्वर एक IP पते के साथ प्रतिक्रिया करता है, और हमारा कम्प्यूटर निस्संदेह इसे वैध प्रतिक्रिया के रूप में स्वीकार करता है और उस वेबसाइट से जुड़ता है। एक DNS लुकअप वास्तव में कई चरणों में होता है। उदाहरण के लिए, जब कोई कम्प्यूटर "www.highereducation.in" के लिए पूछता है, तो DNS लुकअप निम्न कई चरणों में किया जाता है:

- कम्प्यूटर पहले स्थानीय DNS सर्वर (ISP प्रदान) पूछता है। यदि ISP के कैश में यह नाम है, तो यह क्वेरी को "root zone directory" के रूप में अग्रेषित करता है, जहाँ यह ".in" प्राप्त करता है और रूट जोन को उत्तर दे सकता है।
- उत्तर के आधार पर, कम्प्यूटर तब ".in" निर्देशिका पूछता है जहाँ वह "highereducation.in" पा सकता है।
- प्राप्त जानकारी के आधार पर, कम्प्यूटर "highereducation.in" की पूछताछ करता है, जहाँ वह "www.highereducation.in" प्राप्त कर सकता है।

DNS लुकअप, जब DNSSEC का उपयोग करके प्रदर्शित किया जाता है, इसमें प्रतिसाद इकाई द्वारा उत्तरों पर हस्ताक्षर करना सम्मिलित है। DNSSEC सार्वजनिक कुंजी क्रिप्टोग्राफी पर आधारित है।

DNSSEC मानक में, प्रत्येक DNS जोन में एक सार्वजनिक/व्यक्तिगत कुंजी जोड़ी होती है। प्रामाणिकता सुनिश्चित करने के लिए DNS सर्वर द्वारा भेजी गई सभी सूचनाओं की उत्पत्ति क्षेत्र की निजी कुंजी के साथ की जाती है।

DNS ग्राहकों को हस्ताक्षरों की जाँच करने के लिए जोन की सार्वजनिक कुंजियाँ जानना आवश्यक है। सभी शीर्ष–स्तरीय डोमेन या रूट DNS की सार्वजनिक कुंजियों के साथ ग्राहकों को पूर्व–निर्धारित किया जा सकता है।

DNSSEC के साथ, लुकअप प्रक्रिया निम्नानुसार है –

- जब हमारा कम्प्यूटर रूट जोन से पूछता है कि .in कहाँ मिल सकता है, तो उत्तर को रूट जोन सर्वर द्वारा हस्ताक्षरित किया जाता है।

- कम्प्यूटर रूट जोन की हस्ताक्षरित कुंजी का परीक्षण करता है और पुष्टि करता है कि यह सही जानकारी वाला वैध रूट जोन है।
- उत्तर में, रूट जोन .in जोन सर्वर और उसके स्थान के हस्ताक्षर कुंजी पर जानकारी प्रदान करता है, जिससे कम्प्यूटर .in निर्देशिका से संपर्क कर सकता है और यह सुनिश्चित कर सकता है कि यह वैध है।
- .in निर्देशिका तब highereducation.in के लिए हस्ताक्षरित कुंजी और जानकारी प्रदान करता है, जिससे वह google.com से संपर्क कर सकता है और सत्यापित कर सकता है कि हम सही highereducation.in से जुड़े हैं, जैसा कि इसके ऊपर के जोन द्वारा पुष्टि की गई है।
- भेजी गई जानकारी संसाधन रिकॉर्ड सेट (Resource Record Set - RRS) के रूप में है। शीर्ष–स्तरीय .in सर्वर में डोमेन highereducation.in के लिए RRSet का उदाहरण निम्न तालिका में दिखाया गया है।

Domain Name	Time to live	Type	Value
highereducation.in	86400	NS	dns.highereducation.in
dns.highereducation.in	86400	A	36..1.2.3
highereducation.in	86400	KEY	3682793A8B83F831029CE2737D.
highereducation.in	86400	SIG	86947503A7B748F6272E53930C..

- KEY रिकॉर्ड highereducation.in की एक सार्वजनिक कुंजी है।
- SIG रिकॉर्ड शीर्ष स्तर का .in सर्वर के हस्ताक्षरित फील्ड का NS, A और KEY रिकॉर्ड है, जो उनकी प्रामाणिकता को सत्यापित करने के लिए है। इसका मान $Kin_{pvt}(H(NS, A, KEY))$ है।

इस प्रकार, यह माना जाता है कि जब DNSSEC पूरी तरह से रोल आउट (roll out) है, तो उपयोगकर्ता का कम्प्यूटर यह पुष्टि करने में सक्षम है कि DNS प्रतिक्रियाएं वैध और सत्य हैं, और DNS कैश विषाक्तता के माध्यम से लॉन्च किए गए DNS हमलों से बचें।

एप्लीकेशन परत का सार संक्षेपः

ई–मेल हासिल करने की प्रक्रिया संचार की अंत–से–अंत सुरक्षा सुनिश्चित करती है। यह गोपनीयता, प्रेषक प्रमाणीकरण, संदेश अखंडता और गैर–अस्वीकृति की सुरक्षा सेवाएँ प्रदान करता है।

ई–मेल सुरक्षा के लिए दो योजनाएँ विकसित की गई हैंः PGP और S/MIME। ये दोनों योजनाएं गुप्त–कुंजी और सार्वजनिक–कुंजी क्रिप्टोग्राफी का उपयोग करती हैं।

DNS स्पूफिंग/कैश पॉइजनिंग जैसे हमलों के लिए मानक DNS लुकअप असुरक्षित है। DNS लुकअप सुरक्षित करना DNSSEC के उपयोग के माध्यम से संभव है जो सार्वजनिक कुंजी क्रिप्टोग्राफी को कार्य देता है।

अभ्यास

1. ई–मेल सुरक्षा से क्या समझते हैं?
2. ई–मेल सुरक्षा सेवायें क्या हैं?
3. एक–से–एक ई–मेल को समझाइए।
4. एक–से–बहुल प्राप्तकर्ता ई–मेल की अवधारणा को स्पष्ट कीजिए।
5. एक–से–वितरण सूची ई–मेल से क्या समझते हैं?
6. PGP को समझाइए।
7. S/MIME से क्या समझते हैं?
8. DNS सुरक्षा क्या हैं?

अध्याय – 10

ट्रांस्पोर्ट लेयर
(परिवहन परत)

नेटवर्क सुरक्षा हमलों के विरूद्व डेटा हासिल करने पर जोर देती है, जबकि यह एक नेटवर्क पर पारगमन में है। इस लक्ष्य को प्राप्त करने के लिए, कई वास्तविक समय के सुरक्षा प्रोटोकॉल तैयार किए गए हैं। रीयल–टाइम नेटवर्क सुरक्षा प्रोटोकॉल के लिए लोकप्रिय मानक S/MIME, SSL/TLS, SSH और IPsec हैं। जैसा कि पहले उल्लेख किया गया है, ये प्रोटोकॉल नेटवर्किंग मॉडल की विभिन्न परतों पर काम करते हैं।

पूर्व में, हमने कुछ लोकप्रिय प्रोटोकॉल पर चर्चा की, जो एप्लिकेशन परत सुरक्षा प्रदान करने के लिए डिजाइन किए गए हैं। इस अध्याय में, हम ट्रांसपोर्ट परत और संबंधित सुरक्षा प्रोटोकॉल में नेटवर्क सुरक्षा प्राप्त करने की प्रक्रिया पर चर्चा करेंगे।

TCP/IP प्रोटोकॉल आधारित नेटवर्क के लिए, भौतिक और डेटा लिंक परतें आमतौर पर उपयोगकर्ता टर्मिनल और नेटवर्क कार्ड हार्डवेयर में लागू की जाती हैं। ऑपरेटिंग सिस्टम में TCP और IP परतों को लागू किया जाता है। TCP/IP से ऊपर कुछ भी उपयोगकर्ता प्रक्रिया के रूप में लागू किया जाता है।

कम्प्यूटर नेटवर्किंग में, ट्रांसपोर्ट परत इंटरनेट प्रोटोकॉल सूट और OSI मॉडल में नेटवर्क स्टैक में प्रोटोकॉल की स्तरित वास्तुकला में विधियों का एक वैचारिक विभाजन है। इस परत के प्रोटोकॉल अनुप्रयोगों के लिए होस्ट–से–होस्ट संचार सेवाएं प्रदान करते हैं। यह कनेक्शन–उन्मुख संचार, विश्वसनीयता, प्रवाह नियंत्रण और बहुसंकेतन जैसी सेवाएं प्रदान करता है।

TCP/IP मॉडल के ट्रांसपोर्ट परत के कार्यान्वयन और अर्थ का विवरण, जो इंटरनेट की नींव है, और सामान्य नेटवर्किंग का OSI मॉडल पृथक हैं। इंटरनेट के लिए इस परत का उपयोग करने वाले सभी प्रोटोकॉल TCP/IP के विकास में उत्पन्न हुए हैं। OSI मॉडल में ट्रांसपोर्ट परत को अक्सर परत 4, या L4 के रूप में संदर्भित किया जाता है, जबकि संख्यात्मक परत का उपयोग TCP/IP में नहीं किया जाता है।

TCP/IP का सबसे प्रसिद्ध ट्रांस्पोर्ट प्रोटोकॉल ट्रांसमिशन कंट्रोल प्रोटोकॉल (TCP) है, और पूरे सुइट के शीर्षक को इसका नाम दिया गया है। इसका उपयोग कनेक्शन–उन्मुख प्रसारण के लिए किया जाता है, जबकि कनेक्शन रहित यूजर डेटाग्राम प्रोटोकॉल (UDP) का उपयोग सरल संदेश प्रसारण के लिए किया जाता है। विश्वसनीय ट्रांसमिशन और डेटा स्ट्रीम सेवाओं को सम्मिलित करते हुए TCP अधिक जटिल प्रोटोकॉल है। साथ में, TCP और UDP में इंटरनेट पर अनिवार्य रूप से सभी ट्रैफिक सम्मिलित हैं और हर बड़े ऑपरेटिंग सिस्टम में लागू एकमात्र प्रोटोकॉल हैं। परिभाषित और कार्यान्वित की गई अतिरिक्त ट्रांस्पोर्ट परत प्रोटोकॉल में डाटाग्राम कंजेशन कंट्रोल प्रोटोकॉल (DCCP) और स्ट्रीम कंट्रोल ट्रांसमिशन प्रोटोकॉल (SCTP) सम्मिलित हैं।

सेवाएंः

ट्रांसपोर्ट परत सेवाओं को एक प्रोग्रामिंग इंटरफेस के माध्यम से ट्रांसपोर्ट परत प्रोटोकॉल तक पहुँचा दिया जाता है। सेवाओं में निम्नलिखित विशेषताएं सम्मिलित हो सकती हैंः

कनेक्शन–उन्मुख संचारः किसी एप्लिकेशन के लिए अंतर्निहित कनेक्शन–कम मॉडल से निपटने के स्थान पर डेटा स्ट्रीम के रूप में कनेक्शन की व्याख्या करना आसान होता है, जैसे कि यूजर डेटाग्राम प्रोटोकॉल का डेटाग्राम मॉडल और इंटरनेट प्रोटोकॉल।

समान आदेश वितरणः नेटवर्क परत आम तौर पर इस बात का आश्वासन नहीं देता है कि डेटा के पैकेट उसी क्रम में आएंगे जो उन्हें भेजे गए थे, लेकिन अक्सर यह एक वांछनीय विशेषता है। यह आमतौर पर सेगमेंट अंकन के उपयोग के माध्यम से किया जाता है, प्राप्तकर्त्ता उन्हें क्रम में एप्लीकेशन करने के लिए पास करता है। यह हेड–ऑफ–लाइन अवरोध पैदा कर सकता है।

विश्वसनीयताः नेटवर्क की भीड़ और त्रुटियों के कारण परिवहन के दौरान पैकेट खो सकता है। एक चेकसम जैसे त्रुटि पहचान कोड के माध्यम से, परिवहन प्रोटोकॉल यह परीक्षण कर सकता है कि डेटा दूषित नहीं है, और प्रेषक को एक ACK या NAK संदेश भेजकर सही रसीद सत्यापित करें। खोए या दूषित डेटा को फिर से जमा करने के लिए स्वचालित पुनः अनुरोध योजनाओं का उपयोग किया जा सकता है।

प्रवाह नियंत्रणः दो नोड्स के मध्य डेटा ट्रांसमिशन की दर को कभी–कभी एक तेज प्रेषक को रोकने के लिए प्रबंधित करना चाहिए, जिससे डेटा बफर प्राप्त करने से अधिक डेटा प्रेषित किया जा सकता है, जिससे बफर ओवररन हो सकता है। यह रन के तहत बफर को कम करके दक्षता में सुधार करने के लिए भी उपयोग किया जा सकता है।

भीड़ से बचावः भीड़ नियंत्रण दूरसंचार नेटवर्क में यातायात प्रवेश को नियंत्रित कर सकता है, ताकि मध्यवर्ती नोड्स और नेटवर्क के किसी भी प्रसंस्करण या लिंक क्षमताओं के ओवरस्क्रिप्शन से बचने की कोशिश करके और इस तरह के संसाधन कदम उठाने के रूप में भीड़भाड़ से बचने के लिए, पैकेट भेजने की दर कम करने के लिए। उदाहरण के लिए, स्वचालित पुनरावृत्ति अनुरोध नेटवर्क को भीड़भाड़ की स्थिति में रख सकते हैं, इस स्थिति को धीमी शुरुआत सहित प्रवाह नियंत्रण में भीड़ से बचाकर जोड़कर बचा जा सकता है। यह बैंडविड्थ की खपत को ट्रांसमिशन की शुरुआत में या पैकेट रिट्रांसमिशन के बाद कम स्तर पर रखता है।

मल्टीप्लेक्सिंगः पोर्ट एक नोड पर कई एंडपॉइंट प्रदान कर सकते हैं। उदाहरण के लिए, एक डाक पते पर नाम एक प्रकार का बहुसंकेतन है, और एक ही स्थान के विभिन्न प्राप्तकर्ताओं के मध्य अंतर करता है। कम्प्यूटर अनुप्रयोग प्रत्येक अपने स्वयं के पोर्ट पर जानकारी के लिए सुनेंगे, जो एक ही समय में एक से अधिक नेटवर्क सेवा का उपयोग करने में सक्षम बनाता है। यह TCP/IP मॉडल में ट्रांस्पोर्ट परत का भाग है, लेकिन OSI मॉडल में सत्र परत का।

विश्लेषणः

ट्रांसपोर्ट परत होस्ट कम्प्यूटर पर उपयुक्त एप्लिकेशन प्रक्रिया में डेटा पहुंचाने के लिए उत्तरदायी है। इसमें विभिन्न एप्लिकेशन प्रक्रियाओं से डेटा का सांख्यिकीय बहुसंकेतन सम्मिलित होता है, अर्थात डेटा सेगमेंट बनाना, और प्रत्येक ट्रांसपोर्ट लेयर डेटा सेगमेंट के हेडर में स्रोत और गंतव्य पोर्ट संख्याओं को जोड़ना। स्रोत और गंतव्य IP पते के साथ, पोर्ट संख्या एक नेटवर्क सॉकेट का गठन करते हैं, अर्थात् प्रक्रिया से प्रक्रिया संचार का एक पहचान पता। OSI मॉडल में, यह फंक्शन सत्र परत द्वारा समर्थित है।

कुछ ट्रांसपोर्ट परत प्रोटोकॉल, उदाहरण के लिए TCP, लेकिन UDP नहीं, वर्चुअल सर्किट का समर्थन करते हैं, अर्थात् अंतर्निहित पैकेट उन्मुख डेटा नेटवर्क पर कनेक्शन–उन्मुख संचार प्रदान करते हैं। एप्लीकेशन प्रक्रियाओं के लिए पैकेट मोड संचार को छुपाते समय एक बाइट–स्ट्रीम दिया जाता है। इसमें कनेक्शन स्थापना, डेटा स्ट्रीम को पैकेट्स में विभाजित करना सम्मिलित है जिन्हें सेगमेंट कहा जाता है, सेगमेंट क्रमांकन और ऑर्डर डेटा का पुनः क्रमांकन है।

कुछ ट्रांसपोर्ट लेयर प्रोटोकॉल, उदाहरण के लिए TCP, लेकिन UDP नहीं, एंड–टू–एंड (end-to-end) विश्वसनीय संचार प्रदान करते हैं, अर्थात् त्रुटि का पता लगाने के कोड और स्वचालित दोहराने अनुरोध (Automatic Repeat Request - ARQ) प्रोटोकॉल द्वारा त्रुटि की वसूली। ARQ प्रोटोकॉल प्रवाह नियंत्रण भी प्रदान करता है, जिसे कंजेशन से बचा जा सकता है।

UDP एक बहुत ही सरल प्रोटोकॉल है, और न तो वर्चुअल सर्किट और न ही विश्वसनीय संचार प्रदान करता है, इन कार्यों को एप्लीकेशन प्रोग्राम में प्रस्तुत करता है। UDP पैकेट को सेगमेंट के स्थान पर डेटाग्राम कहा जाता है।

TCP का उपयोग कई प्रोटोकॉल के लिए किया जाता है, जिसमें HTTP वेब ब्राउजिंग और ईमेल ट्रांसफर सम्मिलित हैं। यूडीपी का उपयोग मल्टीकास्टिंग और ब्रॉडकास्टिंग के लिए किया जा सकता है, क्योंकि बड़ी मात्रा में मेजबान के लिए रिट्रांसमिशन संभव नहीं है। UDP आमतौर पर उच्च थ्रोपुट और कम विलंबता देता है, और इसलिए इसका उपयोग अक्सर वास्तविक समय मल्टीमीडिया संचार के लिए किया जाता है, जहाँ पैकेट नुकसान को कभी–कभी स्वीकार किया जा सकता है, उदाहरण के लिए IP-TV, IP-telephony और ऑनलाइन कम्प्यूटर गेम के लिए।

कई गैर–आईपी–आधारित नेटवर्क, जैसे कि X.25, Frame Relay और ATM ट्रांस्पोर्ट परत के स्थान पर नेटवर्क या डेटा लिंक परत पर कनेक्शन–उन्मुख संचार को लागू करते हैं। X.25 में, टेलीफोन नेटवर्क मोडेम और वायरलेस संचार प्रणालियों में, निचले प्रोटोकॉल परतों में विश्वसनीय नोड–से–नोड संचार लागू किया जाता है।

OSI कनेक्शन–मोड ट्रांसपोर्ट परत प्रोटोकॉल विनिर्देश ट्रांस्पोर्ट प्रोटोकॉल के पांच वर्गों को परिभाषित करता हैः TP0, जो कम विश्वसनीय नेटवर्क के लिए डिजाइन किया गया है, TP4 को कम से कम त्रुटि रिकवरी प्रदान करता है।

ट्रांसपोर्ट लेयर के उत्तरदायित्वः

1. प्रक्रिया से प्रक्रिया वितरणः

जबकि डेटा लिंक लेयर को एक फ्रेम के MAC एड्रेस (48 बिट्स एड्रेस प्रत्येक होस्ट मशीन के नेटवर्क इंटरफेस कार्ड के अंदर समाहित) की आवश्यकता होती है, एक फ्रेम को सही विधि से वितरित करने के लिए मेजबान होस्ट को पैकेट के उपयुक्त मार्ग के लिए IP एड्रेस की आवश्यकता होती है ट्रांसपोर्ट लेयर को किसी विशेष होस्ट पर चलने वाली कई प्रक्रियाओं के मध्य डेटा के सेगमेंट को सही प्रक्रिया तक सही ढंग से पहुंचाने के लिए एक पोर्ट नंबर की आवश्यकता होती है। पोर्ट नंबर एक 16 बिट एड्रेस है जिसका किसी भी क्लाइंट–सर्वर प्रोग्राम को विशिष्ट रूप से पहचानने के लिए उपयोग किया जाता है।

2. होस्ट के मध्य एंड–टू–एंड कनेक्शनः

ट्रांस्पोर्ट परत होस्ट के मध्य एंड–टू–एंड कनेक्शन बनाने के लिए भी जिम्मेदार है जिसके लिए यह मुख्य रूप से TCP और UDP का उपयोग करता है। TCP एक सुरक्षित, कनेक्शन–उन्मुख प्रोटोकॉल है जो दो सिरों के मध्य एक मजबूत संबंध स्थापित करने के लिए एक हैंडशेक प्रोटोकॉल का उपयोग करता है। TCP संदेशों की विश्वसनीय डिलीवरी सुनिश्चित करता है और इसका उपयोग विभिन्न अनुप्रयोगों में किया जाता है। दूसरी ओर UDP एक सांविधिक और अविश्वसनीय प्रोटोकॉल है जो सर्वोत्तम प्रयास प्रदान करता है। यह उन अनुप्रयोगों के लिए उपयुक्त है, जिनका प्रवाह या त्रुटि नियंत्रण से कोई सरोकार नहीं है और उन्हें वीडियो कॉन्फ्रेंसिंग जैसे डेटा भेजने की आवश्यकता होती है। यह अक्सर मल्टीकास्टिंग प्रोटोकॉल में उपयोग किया जाता है।

3. मल्टीप्लेक्सिंग और डिमल्टिप्लेक्सिंगः

मल्टीप्लेक्सिंग एक नेटवर्क पर विभिन्न अनुप्रयोगों को एक साथ उपयोग की अनुमति देता है जो एक होस्ट पर चल रहे हैं। ट्रांस्पोर्ट परत इस तंत्र को प्रदान करता है जो हमें एक नेटवर्क पर एक साथ विभिन्न अनुप्रयोगों से पैकेट धाराओं को भेजने में सक्षम बनाता है। ट्रांसपोर्ट परत इन पैकेट्स को उनके पोर्ट संख्यां द्वारा विभेदित विभिन्न प्रक्रियाओं से स्वीकार करता है और उचित हेडर जोड़ने के बाद उन्हें नेटवर्क परत में भेजता है। इसी प्रकार विभिन्न प्रक्रियाओं से आने वाले डेटा को प्राप्त करने के लिए प्राप्तकर्त्ता की ओर से डिमल्टिप्लेक्सिंग की आवश्यकता होती है। ट्रांस्पोर्ट नेटवर्क परत से डेटा के खंडों को प्राप्त करता है और इसे उपयोगकर्त्ता की मशीन पर चल रही उचित प्रक्रिया तक पहुँचाता है।

4. भीड़ नियंत्रणः

भीड़भाड़ एक ऐसी स्थिति है जिसमें नेटवर्क पर बहुत से स्रोत डेटा भेजने का प्रयास करते हैं और राउटर बफर ओवरफ्लो होने लगते हैं जिसके कारण पैकेट का नुकसान होता है। परिणामस्वरूप स्रोतों से पैकेट का पुनः प्रसारण करने से भीड़ में और वृद्धि होती है। इस स्थिति में ट्रांसपोर्ट परत विभिन्न विधियों से भीड़ नियंत्रण प्रदान करता है। यह भीड़ नियंत्रण करने के लिए खुले लूप भीड़ नियंत्रण का उपयोग करता है और नेटवर्क से भीड़ समाप्त करने के लिए बंद लूप का उपयोग करता है। भीड़ को नियंत्रित करने के लिए TCP, AIMD (Additive Increase Multiplicative Decrease) की सुविधा प्रदान करता है।

5. डेटा अखंडता और त्रुटि सुधारः

ट्रांसपोर्ट परत, एरर डिटेक्शन कोड, कम्प्यूटिंग चेकसम का उपयोग करके एप्लिकेशन परत से आने वाले संदेशों में त्रुटियों के लिए परीक्षण करता है। यह परीक्षित करता है कि प्राप्त डेटा दूषित नहीं है और डेटा आने और नहीं होने पर प्रेषक को सूचित करने के लिए ACK और NACK सेवाओं का उपयोग करता है या नहीं और डेटा की अखंडता के लिए भी परीक्षण करता है।

6. प्रवाह नियंत्रणः

ट्रांस्पोर्ट परत TCP/IP मॉडल के आसन्न परतों के मध्य एक प्रवाह नियंत्रण तंत्र प्रदान करता है। TCP कुछ प्रवाह नियंत्रण तकनीकों को लगाकर एक तेज प्रेषक और धीमे प्राप्तकर्त्ता के कारण डेटा हानि को भी रोकता है। यह स्लाइडिंग विंडो प्रोटोकॉल की विधि का भी उपयोग करता है जो कि प्राप्तकर्ता द्वारा एक विंडो वापस भेजकर पूरा किया जा सकता है जो डेटा के आकार को सूचित कर सकता है।

10.1 ट्रांस्पोर्ट लेयर (परिवहन परत) सुरक्षा की आवश्यकताः

हम एक विशिष्ट इंटरनेट–आधारित व्यापार लेनदेन की चर्चा करते हैं–

माना सामान बेचने के लिए X, Y की वेबसाइट पर जाता है। वेबसाइट पर एक फॉर्म में, X वांछित और उसके पते और भुगतान कार्ड विवरण के प्रकार और मात्रा प्रविष्ट करता है। X, Submit पर क्लिक करता है और अपने खाते से मूल्य राशि के डेबिट के साथ सामान की डिलीवरी का इंतजार करता है। यह सब अच्छा लगता है, लेकिन नेटवर्क सुरक्षा के अभाव में, X कुछ आश्चर्य के लिए हो सकता है।

यदि लेनदेन गोपनीयता (एन्क्रिप्शन) का उपयोग नहीं करता है, तो एक हमलावर हमारे भुगतान कार्ड की जानकारी प्राप्त कर सकता है। इसके बाद हमलावर X के खर्च पर खरीदारी कर सकता है।

यदि कोई डेटा अखंडता माप का उपयोग नहीं किया जाता है, तो एक हमलावर X के ऑर्डर को प्रकार या सामान की मात्रा के संदर्भ में संशोधित कर सकता है।

अंत में, यदि कोई सर्वर प्रमाणीकरण का उपयोग नहीं किया जाता है, तो एक सर्वर Y के प्रसिद्ध लोगो को प्रदर्शित कर सकता है लेकिन साइट एक दुर्भावनापूर्ण साइट हो सकती है जिसे हमलावर द्वारा बनाए रखा गया हो, जो कि Y के रूप में है। X का आदेश प्राप्त करने के बाद, वह X के पैसे ले सकता था और भाग सकता था या वह X के नाम और क्रेडिट कार्ड के विवरण एकत्र करके एक पहचान की चोरी को अंजाम दे सकता है।

ट्रांसपोर्ट परत सुरक्षा योजना गोपनीयता, डेटा अखंडता, सर्वर प्रमाणीकरण और क्लाइंट प्रमाणीकरण के साथ TCP/IP आधारित नेटवर्क संचार को बढ़ाकर इन समस्याओं को दूर कर सकती है।

इस स्तर पर सुरक्षा का उपयोग ज्यादातर नेटवर्क पर HTTP आधारित वेब लेनदेन को सुरक्षित करने के लिए किया जाता है। हालाँकि, इसे TCP पर चल रहे किसी भी एप्लिकेशन द्वारा नियोजित किया जा सकता है।

TLS डिजाइन का वर्णनः

ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) प्रोटोकॉल TCP परत के ऊपर काम करते हैं। इन प्रोटोकॉल का डिजाइन TCP के लिए लोकप्रिय एप्लिकेशन प्रोग्राम इंटरफेस (API) का उपयोग करता है, जिसे टीसीपी परत के साथ इंटरफेस करने के लिए सॉकेट्स (Sockets) कहा जाता है।

अब एप्लीकेशन सीधे TCP के स्थान पर ट्रांसपोर्ट सिक्योरिटी लेयर से जुड़े हैं। ट्रांसपोर्ट सुरक्षा परत सॉकेट्स के साथ एक साधारण API प्रदान करता है, जो TCP के API के समान और अनुरूप है।

यद्यपि TLS तकनीकी रूप से अनुप्रयोग और परिवहन परत के मध्य रहता है, सामान्य दृष्टिकोण से यह एक ट्रांस्पोर्ट प्रोटोकॉल है जो सुरक्षा सेवाओं के साथ TCP परत के रूप में कार्य करता है।

TLS को TCP पर संचालित करने के लिए, विश्वसनीय परत 4 प्रोटोकॉल (UDP प्रोटोकॉल पर नहीं) को संचालित करने के लिए डिजाइन किया गया है, जिससे TLS का डिजाइन बहुत सरल हो जाता है, क्योंकि इसमें 'timing out' और 'retransmitting lost data' को पुनः प्राप्त करने' के बारे में चिंता करने की आवश्यकता नहीं होती है। TCP परत ऐसा करना जारी रखता है जो सदैव के समान TLS की आवश्यकता को पूरा करता है।

TLS क्यों लोकप्रिय है?

ट्रांसपोर्ट परत पर सुरक्षा का उपयोग करने की लोकप्रियता का कारण सादगी है। इस स्तर पर सुरक्षा के डिजाइन और तैनाती के लिए TCP/IP प्रोटोकॉल में किसी भी परिवर्तन की आवश्यकता नहीं होती है जो एक ऑपरेटिंग सिस्टम में लागू होती है। केवल उपयोगकर्ता प्रक्रियाओं और अनुप्रयोगों को डिजाइन/संशोधित करने की आवश्यकता है जो कम जटिल है।

10.2 सिक्योर सॉकेट लेयर (सुरक्षित सॉकेट परत) (SSL):

सिक्योर सॉकेट्स लेयर (SSL) वेब सर्वर और ब्राउजर के मध्य एन्क्रिप्टेड लिंक स्थापित करने के लिए मानक सुरक्षा तकनीक है। यह लिंक सुनिश्चित करता है कि वेब सर्वर और ब्राउजर के मध्य पारित सभी डेटा निजी और अभिन्न हैं। SSL एक उद्योग मानक है और इसका उपयोग लाखों वेबसाइट्स अपने ग्राहकों के साथ ऑनलाइन लेनदेन के संरक्षण में करती हैं।

SSL कनेक्शन बनाने में सक्षम होने के लिए वेब सर्वर को SSL प्रमाणपत्र की आवश्यकता होती है। जब हम अपने वेब सर्वर पर SSL को सक्रिय करना चुनते हैं, तो हमें अपनी वेबसाइट और हमारी कंपनी की पहचान के बारे में कई सवालों को पूरा करने के लिए प्रेरित किया जाता है। हमारा वेब सर्वर तब दो क्रिप्टोग्राफिक कुंजी बनाता है – एक व्यक्तिगत कुंजी और एक सार्वजनिक कुंजी।

सार्वजनिक कुंजी को गुप्त रखने की आवश्यकता नहीं है और इसे एक प्रमाणपत्र हस्ताक्षर अनुरोध (CSR) में रखा गया है – एक डेटा फाइल जिसमें हमारा विवरण भी है। फिर हमें CSR जमा करना चाहिए। SSL प्रमाणपत्र एप्लीकेशन प्रक्रिया के दौरान, प्रमाणन प्राधिकरण हमारे विवरण को मान्य करेगा और SSL प्रमाणपत्र जारी करेगा जिसमें हमारा विवरण होगा और हमें SSL का उपयोग करने की अनुमति देगा। हमारा वेब सर्वर हमें जारी किए गए SSL प्रमाणपत्र को हमारी व्यक्तिगत कुंजी से सुमेलित करेगा। हमारा वेब सर्वर तब वेबसाइट और हमारे ग्राहक के वेब ब्राउजर के मध्य एक एन्क्रिप्टेड लिंक स्थापित करने में सक्षम होगा।

SSL प्रोटोकॉल की जटिलताएं हमारे ग्राहकों के लिए अदृश्य रहती हैं। इसके स्थान पर उनके ब्राउजर उन्हें एक कुंजी संकेतक प्रदान करते हैं, जिससे उन्हें पता चलता है कि वे वर्तमान में एक SSL एन्क्रिप्टेड सत्र द्वारा संरक्षित हैं – निचले दाएं हाथ के कोने में लॉक आइकन पर क्लिक करने से हमारा SSL प्रमाणपत्र और इसके बारे में विवरण प्रदर्शित होता है। सभी SSL प्रमाणपत्र या तो कंपनियों या कानूनी रूप से जवाबदेह व्यक्तियों को जारी किए जाते हैं।

आमतौर पर एक SSL प्रमाणपत्र में हमारा डोमेन नाम, हमारी कंपनी का नाम, हमारा पता, हमारा शहर, हमारा राज्य और हमारा देश होगा। इसमें प्रमाणपत्र की समाप्ति तिथि भी होगी और प्रमाणपत्र जारी करने के लिए जिम्मेदार प्रमाणन प्राधिकरण का विवरण। जब कोई ब्राउजर किसी सुरक्षित साइट से जुड़ता है तो वह साइट के SSL सर्टिफिकेट को पुनः प्राप्त करेगा और यह परीक्षण करेगा कि यह समाप्त नहीं हुआ है, यह एक प्रमाणीकरण प्राधिकरण द्वारा जारी किया गया है जो ब्राउजर को भरोसा है, और इसका उपयोग उस वेबसाइट द्वारा किया जा रहा है जिसके लिए इसे जारी किया गया है। यदि यह इनमें से किसी एक परीक्षण पर विफल रहता है तो ब्राउजर अंतिम उपयोगकर्ता को एक चेतावनी प्रदर्शित करेगा, जो उन्हें बताएगा कि साइट SSL द्वारा सुरक्षित नहीं है।

SSL का महत्वः

SSL ऐतिहासिक रूप से महत्वपूर्ण है क्योंकि यह पहले व्यापक रूप से उपयोग किया गया था और व्यापक रूप से कार्यान्वित नेटवर्क प्रोटोकॉल था जो पहले से असंबद्ध क्लाइंट और सर्वर सिस्टम के बीच क्रिप्टोग्राफिक रूप से सुरक्षित संचार को सक्षम करने के लिए था।

जबकि SSL नेटस्केप द्वारा डिजाइन और कार्यान्वित एक मालिकाना प्रोटोकॉल के रूप में आरंभ हुआ, वेब सर्वर सॉफ्टवेयर कंपनी ने अपना प्रोटोकॉल प्रकाशित किया और इसे अन्य कंपनियों के लिए लागू करने के लिए उपलब्ध कराया। प्रोटोकॉल को अपने प्रतिद्वंद्वियों के लिए सुलभ बनाकर, नेटस्केप अपने सुरक्षित वेब सर्वर उत्पाद के साथ वेब सर्वर बाजार हिस्सेदारी हासिल करने में सक्षम था, जबकि, एक ही समय में, यह सुनिश्चित करते हुए कि SSL प्रोटोकॉल एक IETF प्रस्तावित मानक बन जाएगा।

SSL को अभी भी लागू किया गया है, अधिकतर विरासत प्रणालियों में, लेकिन अधिकांश दशाओं में, इसे बेहतर सुरक्षा के लिए TLS से बदला जाना चाहिए और पुराने प्रोटोकॉल की कमियों और शोषण से बचना चाहिए।

जबकि प्रोटोकॉल ही अप्रचलित है, SSL कई स्थानों पर रहता है ताकि TLS या SSL का वर्णन किया जा सके ताकि ट्रांस्पोर्ट परत संचार को सुरक्षित किया जा सके। उदाहरण के लिए, प्रमाणपत्र अधिकारी अक्सर अपने वेबसाइट प्रमाणपत्रों को SSL प्रमाणपत्रों के रूप में विपणन करते हैं क्योंकि यह उनके ग्राहकों के लिए अधिक परिचित शब्द है।

SSL कैसे कार्य करता है?

SSL प्रोटोकॉल में दो सबप्रोटोकॉल सम्मिलित हैंः रिकॉर्ड प्रोटोकॉल और हैंडशेक प्रोटोकॉल। हैंडशेक प्रोटोकॉल यह परिभाषित करता है कि कैसे एक वेब क्लाइंट और वेब सर्वर एक SSL कनेक्शन स्थापित करते हैं, जिसमें बातचीत के लिए क्रिप्टोग्राफिक सिस्टम (कूटलेखन प्रणाली) प्रत्येक होस्ट तैयार है – या अनिच्छुक – संचार के लिए उपयोग करने के लिए। SSL क्रिप्टोग्राफिक सामग्री के आदान–प्रदान के लिए प्रक्रियाओं को भी निर्दिष्ट करता है, जैसे कि वेब सर्वर को प्रमाणित करने के लिए SSL प्रमाणपत्र, प्रेषित डेटा के प्रमाणीकरण के लिए सार्वजनिक कुंजी और सत्र एन्क्रिप्शन के लिए निजी कुंजी। रिकॉर्ड प्रोटोकॉल यह परिभाषित करता है कि संचार के लिए डेटा कैसे तैयार किया जाए और रसीद पर इसे सत्यापित या डिक्रिप्ट किया जाए, इसके लिए विशिष्टताओं सहित SSL का उपयोग करके होस्ट डेटा का संचार कैसे करते हैं।

प्रारंभिक हैंडशेक प्रक्रिया के भाग के रूप में, एक सर्वर क्लाइंट को खुद को प्रमाणित करने के लिए अपना SSL प्रमाणपत्र प्रस्तुत करता है। सर्वर प्रमाणपत्र सार्वजनिक कुंजी क्रिप्टोग्राफी मानकों द्वारा परिभाषित X.509 प्रमाणपत्र प्रारूप का पालन करते हैं। प्रमाणीकरण प्रक्रिया डिजिटल प्रमाणपत्र को मान्य करने और यह पुष्टि करने के लिए सार्वजनिक कुंजी एन्क्रिप्शन का उपयोग करती है कि वास्तव में, सर्वर वह होने का दावा करता है। SSL प्रमाणपत्र, किसी भी डिजिटल प्रमाणपत्र की तरह, एक विश्वसनीय प्रमाणपत्र प्राधिकारी द्वारा जारी किया जाना चाहिए।

एक बार सर्वर प्रमाणित हो जाने के उपरान्त, क्लाइंट और सर्वर सत्र की शेष अवधि के दौरान उनके द्वारा विनिमय की गई जानकारी को एन्क्रिप्ट करने के लिए सिफर सेटिंग्स और एक साझा कुंजी स्थापित करते हैं। यह डेटा की गोपनीयता और अखंडता प्रदान करता है। यह पूरी प्रक्रिया उपयोगकर्ता के लिए अदृश्य है। उदाहरण के लिए, यदि किसी वेबपृष्ठ को SSL कनेक्शन की आवश्यकता होती है, तो URL HTTP से HTTP Secure (HTTPS) में बदल जाएगा, और सर्वर के प्रमाणित होते ही ब्राउजर में एक पैडलॉक आइकन दिखाई देगा।

हैंडशेक क्लाइंट को सर्वर पर खुद को प्रमाणित करने की भी अनुमति देता है। इस मामले में, सर्वर प्रमाणीकरण पूरा होने के बाद, ग्राहक को एन्क्रिप्टेड SSL सत्र स्थापित होने से पहले ग्राहक की पहचान प्रमाणित करने के लिए सर्वर को अपना प्रमाण पत्र प्रस्तुत करना होगा।

SSL प्रमाणपत्रः

एसएसएल प्रमाणपत्र सुरक्षित कनेक्शन स्थापित करके विश्वास की नींव बनाते हैं। आगंतुकों को उनका कनेक्शन सुरक्षित होने का आश्वासन देने के लिए, ब्राउजर विशेष दृश्य संकेत प्रदान करते हैं जिन्हें हम EV संकेतक कहते हैं – हरे पैडलॉक से ब्रांडेड URL बार तक कुछ भी।

SSL प्रमाणपत्रों में एक प्रमुख जोड़ी होती हैः एक सार्वजनिक और एक व्यक्तिगत कुंजी। ये कुंजी एक एन्क्रिप्टेड कनेक्शन स्थापित करने के लिए एक साथ काम करती हैं। प्रमाणपत्र में 'विषय' भी सम्मिलित है, जो प्रमाण पत्र/वेबसाइट के मालिक की पहचान है।

प्रमाण पत्र प्राप्त करने के लिए, हमें अपने सर्वर पर प्रमाणपत्र हस्ताक्षर अनुरोध (CSR) बनाना होगा। यह प्रक्रिया हमारे सर्वर पर एक व्यक्तिगत कुंजी और सार्वजनिक कुंजी बनाती है। CSR डेटा फाइल जिसे हम SSL सर्टिफिकेट जारीकर्ता (जिसे सर्टिफिकेट अथॉरिटी या CA कहा जाता है) को भेजते हैं, जिसमें सार्वजनिक कुंजी होती है। CA, CSR डेटा फाइल का उपयोग करता है ताकि वह हमारी व्यक्तिगत कुंजी से सुमेलित किए बिना डेटा संरचना का निर्माण कर सके। CA कभी भी व्यक्तिगत कुंजी नहीं देखता है।

SSL प्रमाणपत्र प्राप्त करने के बाद, हम इसे अपने सर्वर पर स्थापित करते हैं। हम एक मध्यवर्ती प्रमाणपत्र भी स्थापित करते हैं जो हमारे SSL प्रमाणपत्र की विश्वसनीयता को हमारे CA के मूल प्रमाणपत्र से बांधकर स्थापित करता है। हमारे प्रमाणपत्र को स्थापित करने और परीक्षण करने के निर्देश हमारे सर्वर के आधार पर भिन्न होंगे।

SSL प्रमाणपत्र का सबसे महत्वपूर्ण भाग यह है कि यह डिजिटल रूप से एक विश्वसनीय CA द्वारा हस्ताक्षरित है, जैसे DigiCert। कोई भी एक प्रमाण पत्र बना सकता है, लेकिन ब्राउजर केवल उन प्रमाणपत्रों पर भरोसा करते हैं जो किसी संगठन से विश्वसनीय CA की सूची में आते हैं। ब्राउजर विश्वसनीय CA की पूर्व–स्थापित सूची के साथ आते हैं, जिसे विश्वसनीय रूट CA भंडार के रूप में जाना जाता है।

ट्रस्टेड रूट CA भंडार में सम्मिलित होने और इस तरह एक सर्टिफिकेट अथॉरिटी बनने के लिए, एक कंपनी को ब्राउजर्स द्वारा स्थापित सुरक्षा और प्रमाणीकरण मानकों का अनुपालन करना चाहिए। एक संगठन और उसके डोमेन/वेबसाइट को CA द्वारा जारी एक SSL प्रमाणपत्र यह पुष्टि करता है कि एक विश्वसनीय तीसरे पक्ष ने उस संगठन की पहचान को प्रमाणित किया है। चूंकि ब्राउजर CA पर विश्वास करता है, अतः ब्राउजर अब उस संगठन की पहचान पर भी भरोसा करता है। ब्राउजर उपयोगकर्ता को यह जानने देता है कि वेबसाइट सुरक्षित है, और उपयोगकर्ता सुरक्षित ब्राउजिंग को महसूस कर सकता है और यहाँ तक कि अपनी गोपनीय जानकारी भी दर्ज कर सकता है।

यहाँ हम TLS के लिए डिजाइन किए गए प्रोटोकॉल के परिवार पर चर्चा करते हैं। परिवार में SSL संस्करण 2, 3 और TLS प्रोटोकॉल सम्मिलित हैं। SSL2 को अब SSL3 द्वारा बदल दिया गया है, इसलिए हम SSLv3 और TLS पर ध्यान केंद्रित करेंगे।

SSL का संक्षिप्त इतिहासः

वर्ष 1995 में, नेटस्केप ने SSL2 को विकसित किया और नेटस्केप नेविगेटर 1.1 में उपयोग किया। SSL संस्करण 1 कभी भी प्रकाशित और उपयोग नहीं किया गया था। बाद में, माइक्रोसॉफ्ट ने SSL2 में सुधार किया और निजी संचार प्रौद्योगिकी (PCT) नामक एक और समान प्रोटोकॉल पेश किया।

नेटस्केप ने विभिन्न सुरक्षा मुद्दों पर SSL में काफी सुधार किया और 1999 में SSL3 को तैनात किया। इंटरनेट इंजीनियरिंग टास्क फोर्स (IETF) ने बाद में एक समान मानक के रूप में TLS (ट्रांसपोर्ट लेयर सिक्योरिटी) प्रोटोकॉल पेश किया। TLS प्रोटोकॉल SSLv3 के साथ गैर–अंतर–योग्य है।

TLS ने कुंजी विस्तार और प्रमाणीकरण के लिए क्रिप्टोग्राफिक एल्गोरिथ्म को संशोधित किया। इसके अतिरिक्त, TLS ने सुझाव दिया कि SSL में पेटेंट किए गए RSA क्रिप्टो के स्थान पर खुले क्रिप्टो डिफी–हेलमैन और डिजिटल सिग्नेचर स्टैंडर्ड (DSS) का उपयोग किया जाए। लेकिन 2000 में RSA पेटेंट की समाप्ति के कारण, उपयोगकर्ताओं के पास व्यापक रूप से तैनात SSL3 से TLS से दूर स्थानांतरित करने के लिए कोई मजबूत कारण मौजूद नहीं थे।

SSL की मुख्य विशेषताएँः

SSL प्रोटोकॉल की मुख्य विशेषताएँ निम्न हैंः

1. एसएसएल नेटवर्क कनेक्शन सुरक्षा प्रदान करता है।
   - **गोपनीयता** – सूचना का एन्क्रिप्टेड रूप में आदान–प्रदान किया जाता है।
   - **प्रमाणीकरण** – संचार संस्थाएं डिजिटल प्रमाणपत्रों के उपयोग के माध्यम से एक–दूसरे की पहचान करती हैं। वेब–सर्वर प्रमाणीकरण अनिवार्य है जबकि क्लाइंट प्रमाणीकरण को वैकल्पिक रखा गया है।
   - **विश्वसनीयता** – संदेश अखंडता की जांच को बनाए रखता है।
2. एसएसएल सभी TCP अनुप्रयोगों के लिए उपलब्ध है।
3. लगभग सभी वेब ब्राउजर द्वारा समर्थित।
4. नए ऑनलाइन संस्थाओं के साथ व्यापार करने में आसानी प्रदान करता है।
5. मुख्य रूप से वेब ई–कॉमर्स के लिए विकसित।

SSL का आर्किटेक्चरः

SSL, TCP के लिए विशिष्ट है और यह UDP के साथ काम नहीं करता है। SSL अनुप्रयोगों को एप्लीकेशन प्रोग्रामिंग इंटरफेस (API) प्रदान करता है। C और Java, SSL लाइब्रेरी/क्लास आसानी से उपलब्ध हैं।

SSL प्रोटोकॉल को एप्लिकेशन (अनुप्रयोग) और ट्रांसपोर्ट परत के मध्य में हस्तक्षेप करने के लिए डिजाइन किया गया है जैसा कि नीचे दिखाया गया हैः

Application (अनुप्रयोग)	HTTP FTP SMTP
SSL	SSL
TCP	TCP
IP	IP

SSL ही एक एकल परत प्रोटोकॉल नहीं है जैसा कि चित्र में दिखाया गया है। वास्तव में यह दो उप–परतों से बना है। निचली उप–परत में SSL प्रोटोकॉल के एक घटक का समावेश होता है जिसे SSL रिकॉर्ड प्रोटोकॉल कहा जाता है। यह घटक अखंडता और गोपनीयता सेवाएं प्रदान करता है। ऊपरी उप–परत में तीन SSL संबंधित प्रोटोकॉल घटक और एक एप्लिकेशन प्रोटोकॉल सम्मिलित हैं। एप्लिकेशन घटक क्लाइंट/सर्वर इंटरैक्शन के मध्य सूचना हस्तांतरण सेवा प्रदान करता है। तकनीकी रूप से, यह SSL परत के ऊपर भी कार्य कर सकता है। तीन SSL संबंधित प्रोटोकॉल घटक हैं:

- SSL हैंडशेक प्रोटोकॉल (SSL)
- चेंज सिफर स्पेसिफिकेशन प्रोटोकॉल
- अलर्ट प्रोटोकॉल

ये तीनों प्रोटोकॉल सभी SSL संदेश विनिमय का प्रबंधन करते हैं।

SSL प्रोटोकॉल घटकों के कार्य:

SSL प्रोटोकॉल के चार उप–घटक क्लाइंट मशीन और सर्वर के मध्य सुरक्षित संचार के लिए विभिन्न कार्यों को संभालते हैं। वे निम्न हैं:

1. रिकॉर्ड प्रोटोकॉल:

- रिकॉर्ड परत ऊपरी परत प्रोटोकॉल संदेशों को प्रारूपित करता है।
- यह डेटा को प्रबंधनीय ब्लॉक्स (अधिकतम लंबाई 16 KB) में विभाजित करता है। यह वैकल्पिक रूप से डेटा को संपीड़ित करता है।
- डेटा को एन्क्रिप्ट करता है।
- प्रत्येक संदेश के लिए एक हेडर और अंत में एक हैश (संदेश प्रमाणीकरण कोड (MAC)) प्रदान करता है।
- प्रसारण के लिए TCP परत को स्वरूपित ब्लॉकों पर कार्य।

2. SSL हैंडशेक प्रोटोकॉल:

- यह SSL का सबसे जटिल हिस्सा है। किसी भी एप्लिकेशन डेटा को प्रसारित करने से पहले इसे लागू किया जाता है। यह क्लाइंट और सर्वर के मध्य SSL सत्र बनाता है।
- सत्र की स्थापना में सर्वर प्रमाणीकरण, कुंजी और एल्गोरिथ्म वार्ता, स्थापना कुंजी और ग्राहक प्रमाणीकरण (वैकल्पिक) शामिल हैं।
- क्रिप्टोग्राफिक सुरक्षा मापदंडों के अद्वतीय समूह द्वारा एक सत्र की पहचान की जाती है।
- एक ग्राहक और सर्वर के मध्य कई सुरक्षित TCP कनेक्शन समान सत्र साझा कर सकते हैं।
- चार चरणों के माध्यम से हैंडशेक प्रोटोकॉल क्रियाएं होती हैं।

3. चेंज सिफर स्पेसिफिकेशन प्रोटोकॉल:

- SSL प्रोटोकॉल का सबसे सरल हिस्सा। इसमें दो संचार संस्थाओं, क्लाइंट और सर्वर के मध्य एक एकल संदेश का आदान–प्रदान होता है।
- प्रत्येक इकाई चेंज सिफर स्पेक संदेश भेजता है, यह सहमति के अनुसार कनेक्शन की अपनी ओर को सुरक्षित स्थिति में बदल देता है।
- सिफर पैरामीटर लंबित स्थिति को वर्तमान स्थिति में कॉपी किया जाता है।
- इस संदेश का आदान–प्रदान इंगित करता है कि भविष्य के सभी डेटा विनिमय एन्क्रिप्टेड हैं और अखंडता संरक्षित है।

4. SSL अलर्ट प्रोटोकॉल:

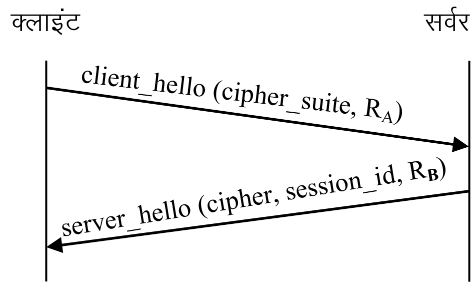
- यह प्रोटोकॉल त्रुटियों को रिपोर्ट करने के लिए उपयोग किया जाता है, जैसे कि अप्रत्याशित संदेश, खराब रिकॉर्ड MAC, सुरक्षा पैरामीटर बातचीत विफल आदि।
- इसका उपयोग अन्य उद्देश्यों के लिए भी किया जाता है, जैसे कि TCP कनेक्शन को बंद करना, खराब या अज्ञात प्रमाण पत्र की सूचना प्राप्त करना, आदि।

SSL सत्र की स्थापनाः

जैसा कि ऊपर चर्चा की गई है, SSL सत्र स्थापना के चार चरण हैं। ये मुख्य रूप से SSL हैंडशेक प्रोटोकॉल द्वारा नियंत्रित किए जाते हैं।

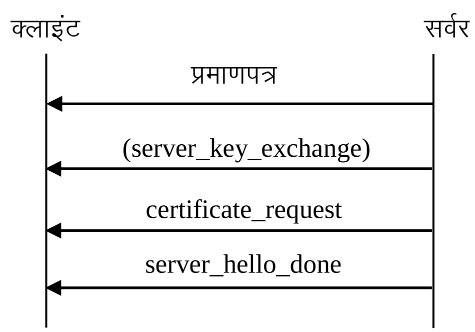
चरण 1: सुरक्षा क्षमताओं की स्थापना।

- इस चरण में दो संदेशों का आदान–प्रदान सम्मिलित है, client_hello और server_hello।
- client_hello में वरीयता के घटते क्रम में क्लाइंट द्वारा समर्थित क्रिप्टोग्राफिक एल्गोरिथ्म (कूटलेखीय कलनविधि) की सूची सम्मिलित है।
- server_hello में चयनित सिफर विर्निदेश और एक नया session_id सम्मिलित है।
- सिफर विर्निदेश में निम्न क्षेत्र सम्मिलित हैं:
  - सिफर एल्गोरिथ्म (कलनविधि) (DES, 3DES, RC2 और RC4)
  - मैक एलगोरिथ्म (कलनविधि) (MD5, SHA-1 पर आधारित)
  - सार्वजनिक कुंजी एल्गोरिथ्म (कलनविधि) (RSA)
  - रिप्ले हमले को रोकने के लिए दोनों संदेशों nonce रखते हैं।



चरण 2: सर्वर प्रमाणीकरण और कुंजी विनिमय।

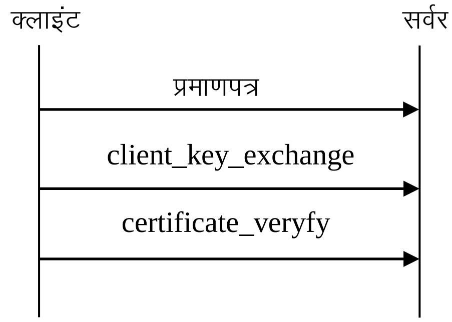
- सर्वर प्रमाण पत्र भेजता है। क्लाइंट सॉफ्टवेयर प्रमाणपत्र के परीक्षण के लिए विभिन्न विश्वसनीय संगठनों (CA) की सार्वजनिक कुंजी के साथ कॉन्फिगर किया गया है।
- सर्वर चुने हुए सिफर सूट भेजता है।
- सर्वर क्लाइंट प्रमाणपत्र का अनुरोध कर सकता है। आमतौर पर ऐसा नहीं किया जाता है।
- सर्वर server_hello के अंत का संकेत देता है।



चरण 3: ग्राहक प्रमाणीकरण और कुंजी विनिमय।

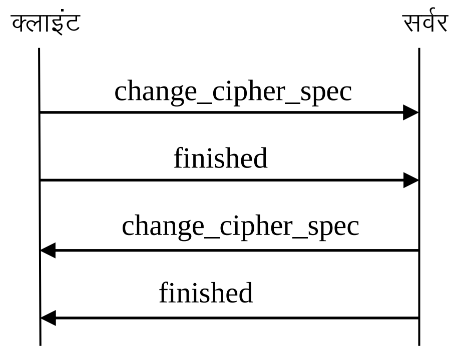
- क्लाइंट प्रमाण पत्र भेजता है, केवल अगर सर्वर द्वारा अनुरोध किया गया हो।
- यह सर्वर की सार्वजनिक कुंजी के साथ एन्क्रिप्टेड प्री–मास्टर सीक्रेट (Pre-Master Secret - PMS) भी भेजता है।

- यदि क्लाइंट इस प्रमाणपत्र के साथ जुड़ी व्यक्तिगत कुंजी रखता है, तो यह साबित करने के लिए कि उसके पास प्रमाण पत्र भेजा गया है, क्लाइंट भी सर्टिफिकेट भेज सकता है। मूल रूप से, क्लाइंट पिछले संदेशों का एक हैश संकेत करता है।



चरण 4: समाप्त।

- क्लाइंट और सर्वर लंबित सिफर स्थिति को वर्तमान स्थिति में कॉपी करने के कारण एक दूसरे को Change_cipher_spec संदेश भेजते हैं।
- अब से, सभी डेटा एन्क्रिप्टेड और अखंडता संरक्षित है।
- प्रत्येक सिरे से संदेश "Finished" सत्यापित करता है कि कुंजी विनिमय और प्रमाणीकरण प्रक्रिया सफल रही।



ऊपर चर्चा किए गए सभी चार चरण TCP सत्र की स्थापना के भीतर होते हैं। SSL सत्र की स्थापना TCP SYN / SYNACK के बाद आरंभ होती है और TCP Fin से पहले पूरी होती है।

एक असम्बद्ध सत्र को फिर से आरंभ करना:

- यदि असम्बद्ध session_id जानकारी के साथ क्लाइंट सर्वर को hello_request भेजता है, तो असम्बद्ध सत्र को फिर से आरंभ करना संभव है।
- सर्वर तब पुनः निर्धारित करता है यदि session_id मान्य हो। यदि मान्य है, तो यह ChangeCipherSpec का आदान–प्रदान करता है और क्लाइंट और सुरक्षित संचार फिर से आरंभ होने के साथ समाप्त संदेश देता है।
- यह सत्र सिफर मापदंडों के पुनर्गणना से बचा जाता है और सर्वर तथा क्लाइंट के अंत में कम्प्यूटिंग को बचाता है।

SSL सत्र कुंजी:

हमने देखा है कि SSL सत्र की स्थापना के चरण 3 के दौरान, क्लाइंट द्वारा सर्वर को सार्वजनिक कुंजी का उपयोग करके एन्क्रिप्ट किए गए सर्वर पर एक प्री–मास्टर सीक्रेट भेजा जाता है। मास्टर सीक्रेट और विभिन्न सत्र कुंजी निम्नानुसार उत्पन्न होती हैं:

- मास्टर सीक्रेट निम्न का उपयोग कर (छद्म यादृच्छिक संख्या जनरेटर के माध्यम से) जनित होता हैः
  - प्री–मास्टर सीक्रेट।
  - दो nonces (RA और RB) client_hello और server_hello संदेशों में विनिमय होते हैं।
- छः गुप्त मान तब इस मास्टर सीक्रेट से व्युत्पन्न होते हैंः
  MAC के साथ उपयोग की जाने वाली गुप्त कुंजी (सर्वर द्वारा भेजे गए डेटा के लिए)
  MAC के साथ उपयोग की जाने वाली गुप्त कुंजी (क्लाइंट द्वारा भेजे गए डेटा के लिए)
  गुप्त कुंजी और IV एन्क्रिप्शन के लिए उपयोग किया जाता है (सर्वर द्वारा)
  गुप्त कुंजी और IV एन्क्रिप्शन के लिए उपयोग किया जाता है (ग्राहक द्वारा)

10.3 TLS प्रोटोकॉल (संदेशाचार) (TLS):

ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) एक प्रोटोकॉल है जो क्लाइंट/सर्वर एप्लिकेशन के मध्य संचार सुरक्षा प्रदान करता है जो इंटरनेट पर एक दूसरे के साथ संचार करते हैं। यह इंटरनेट पर विभिन्न नोड्स के मध्य प्रसारित डेटा के लिए गोपनीयता, अखंडता और सुरक्षा को सक्षम बनाता है। TLS सुरक्षित सॉकेट लेयर (SSL) प्रोटोकॉल का उत्तराधिकारी है।

TLS मुख्य रूप से सुरक्षित वेब ब्राउजिंग, एप्लिकेशन एक्सेस, डेटा ट्रांसफर और अधिकांश इंटरनेट–आधारित संचार को सक्षम बनाता है। यह संचरित/परिवहन किए गए डेटा को छेड़छाड़ होने से रोकता है। TLS का उपयोग वेब ब्राउजर, वेब सर्वर, वीपीएन, डेटाबेस सर्वर और बहुत कुछ सुरक्षित करने के लिए किया जाता है। TLS प्रोटोकॉल में उप–प्रोटोकॉल की दो अलग–अलग परतें होती हैंः

- TLS हैंडशेक प्रोटोकॉलः क्लाइंट और सर्वर को एक दूसरे को प्रमाणित करने और डेटा भेजने से पहले एक एन्क्रिप्शन एल्गोरिथ्म का चयन करने में सक्षम बनाता है।
- TLS रिकॉर्ड प्रोटोकॉलः यह सुनिश्चित करने के लिए मानक TCP प्रोटोकॉल के शीर्ष पर काम करता है कि निर्मित कनेक्शन सुरक्षित और विश्वसनीय है। यह डेटा एनकैप्सुलेशन और डेटा एन्क्रिप्शन सेवाएं भी प्रदान करता है।

TLS प्रोटोकॉल का उद्देश्य मुख्य रूप से दो या अधिक संचार कम्प्यूटर अनुप्रयोगों के मध्य गोपनीयता और डेटा अखंडता प्रदान करना है। TLS द्वारा सुरक्षित क्लाइंट और सर्वर के मध्य कनेक्शन होना चाहिए। वे निम्नलिखित में से एक या अधिक गुण रखते हैंः

- कनेक्शन व्यक्तिगत (या सुरक्षित) है क्योंकि सममित क्रिप्टोग्राफी का उपयोग प्रेषित डेटा को एन्क्रिप्ट करने के लिए किया जाता है। इस सममित एन्क्रिप्शन की कुंजी प्रत्येक कनेक्शन के लिए विशिष्ट रूप से जनित की जाती है और यह एक साझा रहस्य पर आधारित होती है जिसे सत्र की शुरुआत में बातचीत के लिए तैयार किया गया था। सर्वर और क्लाइंट डेटा के पहले बाइट से प्रेषित होने से पहले एन्क्रिप्शन एल्गोरिथ्म और क्रिप्टोग्राफिक कुंजियों का उपयोग करने के विवरण पर बातचीत करते हैं। एक साझा रहस्य की बातचीत दोनों सुरक्षित (बातचीत गुप्त छिपकर काम करने वालों के लिए उपलब्ध नहीं है और प्राप्त नहीं किया जा सकता है, यहाँ तक कि एक हमलावर जो खुद को कनेक्शन के बीच में रखता है) और विश्वसनीय (कोई भी हमलावर बिना बातचीत के संचार को संशोधित नहीं कर सकता है) हैं।
- सार्वजनिक कुंजी क्रिप्टोग्राफी का उपयोग करके संचार पक्षों की पहचान को प्रमाणित किया जा सकता है। इस प्रमाणीकरण को वैकल्पिक बनाया जा सकता है, लेकिन आमतौर पर कम से कम एक पक्ष (आमतौर पर सर्वर) के लिए आवश्यक होता है।
- कनेक्शन विश्वसनीय है क्योंकि प्रसारित किए गए प्रत्येक संदेश में प्रसारण के माध्यम से डेटा के अवांछित नुकसान या परिवर्तन को रोकने के लिए एक संदेश प्रमाणीकरण कोड का उपयोग करके एक संदेश अखंडता का परीक्षण सम्मिलित है।

उपरोक्त गुणों के अतिरिक्त, TLS का सावधानीपूर्वक कॉन्फिगरेशन अतिरिक्त गोपनीयता से संबंधित गुण प्रदान कर सकता है जैसे कि आगे की गोपनीयता, यह सुनिश्चित करना कि एन्क्रिप्शन कुंजी के किसी भी भविष्य के प्रकटीकरण का उपयोग पूर्व में प्रविष्ट किसी भी TLS संचार को डिक्रिप्ट करने के लिए नहीं किया जा सकता है।

TLS कुंजियों के आदान–प्रदान, डेटा को एन्क्रिप्ट करने और संदेश की अखंडता को प्रमाणित करने के लिए कई पृथक–पृथक विधियों का समर्थन करता है। परिणामस्वरूप, TLS के सुरक्षित कॉन्फिगरेशन में कई कॉन्फिगरेशन पैरामीटर सम्मिलित हैं, और सभी विकल्प उपरोक्त सूची में वर्णित सभी गोपनीयता–संबंधित गुणों को प्रदान नहीं करते हैं।

TLS प्रदान करने के लिए संचार सुरक्षा के पहलुओं को हटाने के प्रयास किए गए हैं, और इन सुरक्षा खतरों को संबोधित करने के लिए प्रोटोकॉल को कई बार संशोधित किया गया है। वेब ब्राउजर्स के डेवलपर्स ने इन्हे खोजे जाने के उपरान्त संभावित सुरक्षा कमजोरियों से बचाव के लिए अपने उत्पादों को भी संशोधित किया है।

TLS प्रोटोकॉल में दो परतें शामिल हैं: TLS रिकॉर्ड और TLS हैंडशेक प्रोटोकॉल।

SSL का एक खुला इंटरनेट मानक प्रदान करने के लिए, IETF ने जनवरी 1999 में ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) प्रोटोकॉल जारी किया। TLS को RFC 5246 में प्रस्तावित इंटरनेट मानक के रूप में परिभाषित किया गया है।

मुख्य विशेषताएं:

TLS प्रोटोकॉल में SSL के समान उद्देश्य हैं।

यह क्लाइंट/सर्वर एप्लिकेशन को प्रमाणित करने के लिए एक सुरक्षित तरीके से संवाद करने में सक्षम बनाता है, हमलों को रोकने और संदेश संशोधन का विरोध करने के लिए यह सक्षम है।

TLS प्रोटोकॉल नेटवर्किंग परतों में विश्वसनीय कनेक्शन–उन्मुख परिवहन TCP परत के ऊपर बैठता है।

TLS प्रोटोकॉल की वास्तुकला SSLv3 प्रोटोकॉल के समान है। इसके दो उप प्रोटोकॉल हैं: TLS रिकॉर्ड प्रोटोकॉल और TLS हैंडशेक प्रोटोकॉल।

हालांकि SSLv3 और TLS प्रोटोकॉल में समान वास्तुकला है, विशेष रूप से हैंडशेक प्रोटोकॉल के लिए वास्तुकला और कार्यप्रणाली में कई बदलाव किए गए थे।

TLS और SSL प्रोटोकॉल की तुलना:

TLS और SSLv3 प्रोटोकॉल के मध्य मुख्य आठ अंतर हैं। ये निम्न प्रकार हैं:

1. प्रोटोकॉल संस्करण: TLS प्रोटोकॉल सेगमेंट का हैडर SSL प्रोटोकॉल खंड हेडर द्वारा किए गए नंबर 3 के मध्य अंतर करने के लिए संस्करण संख्या 3.1 को वहन करता है।

2. संदेश प्रमाणीकरण: TLS एक कुंजी–हैश संदेश प्रमाणीकरण कोड (H-MAC) नियुक्त करता है। लाभ यह है कि H-MAC केवल MD5 या SHA के साथ किसी भी हैश फंक्शन के साथ संचालित होता है, जैसा कि SSL प्रोटोकॉल द्वारा स्पष्ट रूप से कहा गया है।

3. सत्र कुंजी जनन: मुख्य सामग्री के निर्माण के लिए TLS और SSL प्रोटोकॉल के मध्य दो अंतर हैं।

- प्री–मास्टर और मास्टर रहस्यों की गणना करने की विधि समान है। लेकिन TLS प्रोटोकॉल में, मास्टर सीक्रेट की गणना एड–हॉक MAC के स्थान पर HMAC मानक और छद्म आयामी फंक्शन (PRF) आउटपुट का उपयोग करती है।
- कंप्यूटिंग प्रोटोकॉल के लिए एल्गोरिथ्म सत्र कुंजी और प्रारंभिक मान (IV) SSL प्रोटोकॉल की तुलना में TLS में अलग है।

4. चेतावनी प्रोटोकॉल संदेश:

- TLS प्रोटोकॉल SSL के अलर्ट प्रोटोकॉल द्वारा उपयोग किए जाने वाले सभी संदेशों का समर्थन करता है, बिना किसी सर्टिफिकेट अलर्ट संदेश को बेमानी किए जाने के अतिरिक्त। क्लाइंट खाली प्रमाणपत्र भेजता है यदि ग्राहक प्रमाणीकरण आवश्यक नहीं है।
- अन्य त्रुटि स्थितियों जैसे कि record_overflow, decode_error आदि के लिए TLS प्रोटोकॉल में कई अतिरिक्त अलर्ट संदेश सम्मिलित किए गए हैं।

5. समर्थित सिफर सूटः SSL RSA, डिफी–हेलमैन और फोर्टाजा साइफर सुइट्स का समर्थन करता है। TLS प्रोटोकॉल फोर्टेजा के अतिरिक्त सभी सूटों का समर्थन करता है।

6. क्लाइंट सर्टिफिकेट प्रकारः TLS सर्टिफिकेट प्रकार को certificate_request संदेश में प्रार्थना करता है। SSLv3 इन सभी का समर्थन करता है। इसके अतिरिक्त, SSL कुछ अन्य प्रकार के प्रमाण पत्र जैसे कि Fortezza का समर्थन करता है।

7. प्रमाणपत्र सत्यापन और समाप्त संदेशः

- SSL में, जटिल संदेश प्रक्रिया का उपयोग सर्टिफिकेट के लिए किया जाता है। TLS के साथ, सत्यापित जानकारी इस जटिल प्रक्रिया से बचने के लिए हैंडशेक संदेशों में ही निहित है।
- समाप्त संदेश TLS और SSLv3 में अलग–अलग शिष्टाचार में गणना की जाती है।

8. डेटा की पैडिंगः SSL प्रोटोकॉल में, एन्क्रिप्शन से पहले उपयोगकर्ता डेटा में जोड़ा गया पैडिंग, कुल डेटा आकार को सिफर की ब्लॉक लंबाई के कई के बराबर बनाने के लिए आवश्यक न्यूनतम मान है। TLS में, पैडिंग किसी भी मात्रा का हो सकत है जो डेटा आकार के परिणामस्वरूप होता है, जो सिफर के ब्लॉक की लंबाई से अधिकतम 255 बाइट्स तक होता है।

TLS कैसे कार्य करता है?

TLS का उपयोग TCP जैसे ट्रांसपोर्ट परत सुरक्षा प्रोटोकॉल के शीर्ष पर किया जा सकता है। TLS में तीन मुख्य घटक हैंः एन्क्रिप्शन, प्रमाणीकरण और अखंडता।

एन्क्रिप्शनः तीसरे पक्ष से स्थानांतरित किए जा रहे डेटा को छुपाता है।

प्रमाणीकरणः यह सुनिश्चित करता है कि सूचनाओं का आदान–प्रदान करने वाले पक्ष वे हैं जो वे होने का दावा करते हैं।

अखंडताः सत्यापित करता है कि डेटा नकली या छेड़छाड़ नहीं किया गया है।

TLS कनेक्शन को TLS हैंडशेक के रूप में ज्ञात अनुक्रम का उपयोग करके आरंभ किया जाता है। TLS हैंडशेक प्रत्येक संचार सत्र के लिए एक साइबर सुइट की स्थापना करता है। सायबर सुइट एल्गोरिथ्म का एक समूह है जो विवरण को निर्दिष्ट करता है जैसे कि साझा एन्क्रिप्शन कुंजियाँ या सत्र कुंजियाँ, उस विशेष सत्र के लिए उपयोग की जाएंगी। TLS एक अनएन्क्रिप्टेड चैनल की तुलना में सुमेलन सत्र कुंजी को व्यवस्थित करने में सक्षम है, जिसे सार्वजनिक कुंजी क्रिप्टोग्राफी के रूप में जाना जाता है।

हैंडशेक प्रमाणीकरण को भी हैंडल करता है, जिसमें आमतौर पर क्लाइंट को अपनी पहचान साबित करने वाले सर्वर होते हैं। यह सार्वजनिक कुंजी का उपयोग करके किया जाता है। सार्वजनिक कुंजी एन्क्रिप्शन कुंजियाँ हैं जो एक तरफा एन्क्रिप्शन का उपयोग करती हैं, जिसका अर्थ है कि कोई भी अपनी प्रामाणिकता सुनिश्चित करने के लिए व्यक्तिगत कुंजी के साथ एन्क्रिप्ट किए गए डेटा को अनचाहा कर सकता है, लेकिन केवल मूल प्रेषक व्यक्तिगत कुंजी के साथ डेटा एन्क्रिप्ट कर सकता है।

एक बार डेटा एन्क्रिप्ट और प्रमाणित हो जाने के उपरान्त, इसे फिर एक मैसेज ऑथेंटिकेशन कोड (MAC) के साथ हस्ताक्षर किया जाता है। प्राप्तकर्ता तब MAC को सत्यापित कर सकता है ताकि डेटा की अखंडता सुनिश्चित हो सके।

TLS सुरक्षाः

सिक्योर सॉकेट्स लेयर (SSL) और ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) क्रिप्टोग्राफिक सुरक्षा प्रोटोकॉल हैं। उनका उपयोग यह सुनिश्चित करने के लिए किया जाता है कि नेटवर्क संचार सुरक्षित है। उनका मुख्य लक्ष्य डेटा अखंडता और संचार गोपनीयता प्रदान करना है। SSL प्रोटोकॉल इस उद्देश्य के लिए डिजाइन किया गया पहला प्रोटोकॉल था और TLS इसका उत्तराधिकारी है। SSL अब अप्रचलित और असुरक्षित माना जाता है (यहां तक कि इसके नवीनतम संस्करण भी), इसलिए क्रोम या फायरफॉक्स जैसे आधुनिक ब्राउजर TLS का उपयोग करते हैं।

SSL और TLS आमतौर पर वेब ब्राउजर द्वारा वेब एप्लिकेशन और वेब सर्वर के मध्य कनेक्शन की रक्षा के लिए उपयोग किए जाते हैं। कई अन्य TCP आधारित प्रोटोकॉल TLS/SSL के साथ–साथ ईमेल (SMTP/POP3), इंस्टेंट मैसेजिंग (XMPP), FTP, VOIP, VPN और अन्य का उपयोग करते हैं।

आमतौर पर, जब कोई सेवा एक सुरक्षित कनेक्शन का उपयोग करती है, तो S प्रोटोकॉल नाम के अक्षर से जुड़ा होता है, उदाहरण के लिए, HTTPS, SMTPS, FTPS, SIPS। अधिकांश दशाओं में, SSL/TLS कार्यान्वयन ओपन SSL पुस्तकालय पर आधारित हैं।

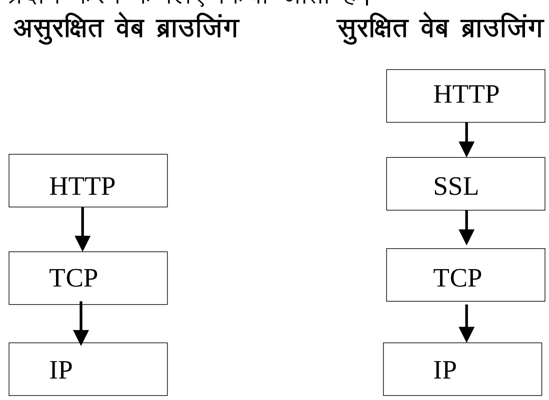
SSL और TLS ऐसे फ्रेमवर्क हैं जो विभिन्न क्रिप्टोग्राफिक एल्गोरिथ्म का उपयोग करते हैं, उदाहरण के लिए, RSA और विभिन्न डिफी–हेलमैन एल्गोरिथ्म। पक्ष प्रारंभिक संचार के दौरान किस एल्गोरिथ्म का उपयोग करने पर सहमत हैं। नवीनतम TLS संस्करण (TLS 1.3) IETF (Internet Engineering Task Force) दस्तावेज RFC 8446 में निर्दिष्ट है और नवीनतम SSL संस्करण (SSL 3.0) IETF दस्तावेज RFC 6101 में निर्दिष्ट है।

10.4 सिक्योर (सुरक्षित) ब्राउजिंग – HTTPS:

इस अनुच्छेद में, हम सुरक्षित वेब ब्राउजिंग करने के लिए SSL/TLS प्रोटोकॉल के उपयोग पर चर्चा करेंगे।

HTTPS परिभाषितः

वेब ब्राउजिंग के लिए हाइपर टेक्स्ट ट्रांसफर प्रोटोकॉल (HTTP) प्रोटोकॉल का उपयोग किया जाता है। HTTPS का कार्य HTTP के समान है। अंतर केवल इतना है कि HTTPS सुरक्षित वेब ब्राउजिंग प्रदान करता है। इस प्रोटोकॉल का उपयोग क्लाइंट वेब ब्राउजर और वेबसाइट सर्वर के बीच एन्क्रिप्टेड और प्रामाणिक कनेक्शन प्रदान करने के लिए किया जाता है।



(चित्र क्र0 10.1)

HTTPS के माध्यम से सुरक्षित ब्राउजिंग सुनिश्चित करता है कि निम्नलिखित सामग्री एन्क्रिप्टेड है:

- अनुरोधित वेब पेज का URL।
- वेब पेज की सामग्री उपयोगकर्ता क्लाइंट को सर्वर द्वारा प्रदान की जाती है।
- उपयोगकर्ता द्वारा भरे गए प्रपत्रों की सामग्री।
- कुकीज दोनों दिशाओं में स्थापित।

HTTPS की कार्यप्रणालीः

HTTPS एप्लीकेशन प्रोटोकॉल आमतौर पर दो लोकप्रिय ट्रांसपोर्ट लेयर सिक्योरिटी प्रोटोकॉल में से एक – SSL या TLS का उपयोग करता है। सुरक्षित ब्राउजिंग की प्रक्रिया निम्नलिखित बिंदुओं में वर्णित है।

- हम https: // और उसके बाद ब्राउजर एड्रेस बार में URL दर्ज करके एक वेबपेज के लिए HTTPS कनेक्शन का अनुरोध करते हैं।

- वेब ब्राउजर वेब सर्वर से कनेक्शन शुरू करता है।
- इस दशा में एक एप्लीकेशन ब्राउजर, पोर्ट 80 के स्थान पर सिस्टम पोर्ट 443 (http के मामले में उपयोग किया जाता है) का उपयोग करता है।
- SSL प्रोटोकॉल एक सुरक्षित सत्र की स्थापना के लिए एक हैंडशेक प्रोटोकॉल से गुजरता है जैसा कि पूर्व अनुच्छेदों में चर्चा की गई थी।
- वेबसाइट आरंभ में अपना SSL डिजिटल सर्टिफिकेट हमारे ब्राउजर को भेजता है। प्रमाणपत्र के सत्यापन पर, SSL हैंडशेक सत्र के लिए साझा रहस्यों का आदान–प्रदान करने के लिए आगे बढ़ता है।
- जब एक विश्वसनीय SSL डिजिटल प्रमाणपत्र सर्वर द्वारा उपयोग किया जाता है, तो उपयोगकर्ताओं को ब्राउजर एड्रेस बार में एक पैडलॉक आइकॉन देखने को मिलता है। जब किसी वेबसाइट पर एक विस्तारित सत्यापन प्रमाणपत्र स्थापित किया जाता है, तो एड्रेस बार हरा हो जाता है।
- एक बार सत्र स्थापित होने के उपरान्त, इस सत्र में वेब सर्वर और ब्राउजर के मध्य कई सुरक्षित कनेक्शन होते हैं।

HTTPS का उपयोगः

HTTPS का उपयोग उपयोगकर्ता को गोपनीयता, सर्वर प्रमाणीकरण और संदेश अखंडता प्रदान करता है। यह इंटरनेट पर ई–कॉमर्स के सुरक्षित संचालन को सक्षम बनाता है।
डेटा को हमलों से बचाता है और पहचान की चोरी से इनकार करता है जो HTTP पर आम हमले हैं।

वर्तमान समय में वेब ब्राउजर और वेब सर्वर HTTPS का समर्थन करते हैं। HTTP पर HTTPS का उपयोग, हालांकि, क्लाइंट पर अधिक कम्प्यूटिंग शक्ति की आवश्यकता होती है और एन्क्रिप्शन तथा SSL हैंडशेक को अंजाम देने के लिए सर्वर सिरे की आवश्यकता होती है।

हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल सिक्योर (HTTPS) हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल (HTTP) का विस्तार है। इसका उपयोग कम्प्यूटर नेटवर्क पर सुरक्षित संचार के लिए किया जाता है, और इंटरनेट पर इसका व्यापक रूप से उपयोग किया जाता है। HTTPS में, संचार प्रोटोकॉल ट्रांसपोर्ट लेयर सिक्योरिटी (TLS), या, पूर्व में, इसके पूर्ववर्ती, सिक्योर सॉकेट्स लेयर (SSL) का उपयोग करके एन्क्रिप्ट किया गया है। इसलिए प्रोटोकॉल को अक्सर TLS पर HTTP या SSL पर HTTP के रूप में भी जाना जाता है।

HTTPS के लिए मुख्य प्रेरणा पहुँच वाली वेबसाइट का प्रमाणीकरण है और पारगमन के दौरान विनिमय किए गए डेटा की गोपनीयता और अखंडता की सुरक्षा है। यह बीच–बीच में होने वाले हमलों से बचाता है। क्लाइंट और सर्वर के मध्य संचार का द्विदिश एन्क्रिप्शन, एन्क्रिप्शन के संचार की छेड़छाड़ से बचाता है। व्यवहार में, यह एक उचित आश्वासन प्रदान करता है कि एक हमलावर द्वारा वेबसाइट के साथ हस्तक्षेप किए बिना संचार कर रहा है, जिसका उद्देश्य किसी फ्राड के विपरीत संवाद करना है।

ऐतिहासिक रूप से, HTTPS कनेक्शन मुख्य रूप से वर्ल्ड वाइड वेब, ई–मेल पर भुगतान लेनदेन और कॉर्पोरेट सूचना प्रणालियों में संवेदनशील लेनदेन के लिए उपयोग किया जाता था। 2018 के बाद से, HTTPS मूल गैर–सुरक्षित HTTP की तुलना में वेब उपयोगकर्ताओं द्वारा अधिक बार उपयोग किया जाता है, मुख्य रूप से सभी प्रकार की वेबसाइट्स पर पृष्ठ प्रामाणिकता की रक्षा करने के लिए, सुरक्षित खाते और उपयोगकर्ता संचार, पहचान और वेब ब्राउजिंग को व्यक्तिगत रखें।

HTTP से अंतरः

HTTPS URL "https: //" से शुरू होते हैं और डिफॉल्ट रूप से पोर्ट 443 का उपयोग करते हैं, जबकि HTTP URL "http: //" से शुरू होते हैं और डिफॉल्ट रूप से पोर्ट 80 का उपयोग करते हैं।

HTTP एन्क्रिप्टेड नहीं है और मैन–इन–द–मिडिल और किसी अन्य व्यक्ति के हमलों के लिए असुरक्षित है, जो हमलावरों को वेबसाइट खातों और संवेदनशील जानकारी तक पहुँच प्राप्त कर सकते हैं, और मैलवेयर या विज्ञापनों को इंजेक्ट करने के लिए वेबपृष्ठों को संशोधित कर सकते हैं। HTTPS को ऐसे हमलों का सामना करने के लिए डिजाइन किया गया है और उनके विरूद्ध सुरक्षित (SSL के पुराने, हटाए गए संस्करणों के अपवाद के साथ) माना जाता है।

नेटवर्क परतः

HTTP, TCP/IP मॉडल की उच्चतम परत पर काम करता है, एप्लिकेशन परत, जैसा कि TLS सुरक्षा प्रोटोकॉल (एक ही परत के निचले उपपरत के रूप में परिचालन) करता है, जो ट्रांसमिशन से पहले एक HTTP संदेश को एन्क्रिप्ट करता है और आगमन पर एक संदेश को डिक्रिप्ट करता है। HTTPS एक अलग प्रोटोकॉल नहीं है, लेकिन एक एन्क्रिप्टेड SSL/TLS कनेक्शन पर साधारण HTTP के उपयोग को संदर्भित करता है।

HTTPS, HTTP हेडर और अनुरोध/प्रतिक्रिया डेटा सहित सभी संदेश सामग्री को एन्क्रिप्ट करता है। नीचे दिए गए सीमाओं में वर्णित संभावित CCA क्रिप्टोग्राफिक हमले के अपवाद के साथ, एक हमलावर को केवल यह पता लगाने में सक्षम होना चाहिए कि दो पक्षों और उनके डोमेन नाम और IP पते के बीच एक कनेक्शन हो रहा है।

सीमाएंः

SSL और TLS एन्क्रिप्शन को दो मोड में कॉन्फिगर किया जा सकता हैः सरल और पारस्परिक। सरल मोड में, प्रमाणीकरण केवल सर्वर द्वारा किया जाता है। पारस्परिक संस्करण को उपयोगकर्ता को उपयोगकर्ता प्रमाणीकरण के लिए वेब ब्राउजर में एक व्यक्तिगत क्लाइंट प्रमाणपत्र स्थापित करने की आवश्यकता होती है। सुरक्षा का स्तर सॉफ्टवेयर के कार्यान्वयन की सहीता और उपयोग में क्रिप्टोग्राफिक एल्गोरिथ्म पर निर्भर करता है।

SSL/TLS वेब क्रॉलर द्वारा साइट के अनुक्रमण को नहीं रोकता है, और कुछ मामलों में एन्क्रिप्टेड संसाधन का URI केवल एन्क्रिप्टेड अनुरोध/प्रतिक्रिया आकार को जानकर पता लगाया जा सकता है। यह एक हमलावर को क्रिप्टोग्राफिक हमले की अनुमति देते हुए प्लेन–टेक्स्ट (सार्वजनिक रूप से उपलब्ध स्थिर सामग्री), और एन्क्रिप्टेड टेक्स्ट (स्थिर सामग्री का एन्क्रिप्टेड संस्करण) तक पहुँचने की अनुमति देता है।

क्योंकि TLS, HTTP के नीचे एक प्रोटोकॉल स्तर पर चल रहा है, और उच्च्य स्तर के प्रोटोकॉल का कोई ज्ञान नहीं है, TLS सर्वर केवल एक विशेष पते और पोर्ट संयोजन के लिए सख्ती से एक प्रमाण पत्र प्रस्तुत कर सकते हैं। पूर्व में, इसका अर्थ यह था कि HTTPS के साथ नाम–आधारित वर्चुअल होस्टिंग का उपयोग करना संभव नहीं था। सर्वर नेम इंडिकेशन (SNI) नामक एक हल उपलब्ध है, जो कनेक्शन को एन्क्रिप्ट करने से पहले होस्ट नाम को सर्वर पर भेजता है। हालांकि कई पुराने ब्राउजर इस विस्तार का समर्थन नहीं करते हैं। SNI के लिए समर्थन फायरफॉक्स 2, ओपेरा 8, सफारी 2.1, गूगल क्रोम 6 और विंडोज विस्टा पर इंटरनेट एक्सप्लोरर 7 के बाद से उपलब्ध है।

वास्तुकला की दृष्टि सेः

- एक SSL/TLS कनेक्शन को प्रथम फ्रंट मशीन द्वारा प्रबंधित किया जाता है जो TLS कनेक्शन आरंभ करता है। यदि, किसी भी कारण (रूटिंग, ट्रैफिक ऑप्टिमाइजेशन, आदि) के लिए, यह फ्रंट मशीन एप्लिकेशन सर्वर नहीं है और इसे डेटा को डिक्रिप्ट करना है, तो एप्लिकेशन सर्वर को उपयोगकर्ता प्रमाणीकरण जानकारी या प्रमाण पत्र का प्रचार करने के लिए समाधान खोजना होगा, जिसकी आवश्यकता है पता है कि कौन कनेक्ट होने जा रहा है।
- SSL/TLS के लिए आपसी प्रमाणीकरण के साथ, SSL/TLS सत्र पहले सर्वर द्वारा प्रबंधित किया जाता है जो कनेक्शन शुरू करता है। उन परिस्थितियों में जहाँ एन्क्रिप्शन को श्रृंखलित सर्वर के साथ प्रचारित किया जाना है, सत्र समय पर प्रबंधन को लागू करने के लिए बेहद मुश्किल हो जाता है।
- आपसी SSL/TLS के साथ, सुरक्षा अधिकतम है, लेकिन क्लाइंट सिरे पर, SSL/TLS कनेक्शन को ठीक से समाप्त करने की कोई विधि नहीं है और सभी संबंधित क्लाइंट अनुप्रयोगों को समाप्त करने या बंद करने के लिए सर्वर सत्र की प्रतीक्षा करके उपयोगकर्ता को डिस्कनेक्ट करें।

HTTPS के लाभः

सुरक्षित संचारः HTTPS ब्राउजर और सर्वर या किसी भी दो सिस्टम के मध्य एक एन्क्रिप्टेड लिंक स्थापित करके एक सुरक्षित कनेक्शन बनाता है।

डेटा अखंडताः HTTPS डेटा एन्क्रिप्ट करके डेटा अखंडता प्रदान करता है और इसलिए, भले ही हैकर्स डेटा को पाने का प्रबंधन करते हैं, वे इसे पढ़ या संशोधित नहीं कर सकते हैं।

गोपनीयता और सुरक्षाः HTTPS ब्राउजर और सर्वर के मध्य संचार सुनने के लिए हैकर्स को रोककर वेबसाइट उपयोगकर्ताओं की गोपनीयता और सुरक्षा की रक्षा करता है।

तीव्र प्रदर्शनः HTTPS डेटा के आकार को एन्क्रिप्ट और कम करके HTTP की तुलना में डेटा ट्रांसफर की गति को बढ़ाता है।

SEO: HTTPS का उपयोग SEO रैंकिंग को बढ़ाता है। गूगल क्रोम में, यदि उपयोगकर्ता का डेटा HTTP पर एकत्र किया जाता है, तो गूगल ब्राउजर में Not Secure लेबल दिखाता है।

भविष्यः HTTPS उपयोगकर्ताओं और वेबसाइट के मालिकों के लिए इंटरनेट को सुरक्षित बनाकर वेब के भविष्य का प्रतिनिधित्व करता है।

10.5 सिक्योर शेल प्रोटोकॉल (सुरक्षित शेल संदेशाचार) (SSH)

सुरक्षित शेल (SSH) एक असुरक्षित नेटवर्क पर सुरक्षित रूप से नेटवर्क सेवाओं के संचालन के लिए एक क्रिप्टोग्राफिक नेटवर्क प्रोटोकॉल है। विशिष्ट अनुप्रयोगों में दूरस्थ कमांड–लाइन लॉगिन और दूरस्थ कमांड निष्पादन शामिल हैं, लेकिन SSH के साथ किसी भी नेटवर्क सेवा को सुरक्षित किया जा सकता है।

SSH एक क्लाइंट नेटवर्क सर्वर में एक असुरक्षित नेटवर्क पर एक सुरक्षित चैनल प्रदान करता है, जो SSH सर्वर के साथ SSH क्लाइंट एप्लिकेशन को जोड़ता है। प्रोटोकॉल विनिर्देश SSH–1 और SSH–2 के रूप में संदर्भित दो प्रमुख संस्करणों के मध्य अंतर करता है। SSH के लिए मानक TCP पोर्ट 22 है। SSH का उपयोग आमतौर पर यूनिक्स जैसे ऑपरेटिंग सिस्टम तक पहुँचने के लिए किया जाता है, लेकिन इसका उपयोग माइक्रोसॉफ्ट विंडोज के लिए भी किया जा सकता है। विंडोज 10 ओपन SSH को अपने डिफॉल्ट SSH क्लाइंट के रूप में उपयोग करता है।

SSH को टेलनेट के लिए एक प्रतिस्थापन के रूप में और असुरक्षित रिमोट शेल प्रोटोकॉल जैसे कि बर्कले rlogin, rsh और rexec प्रोटोकॉल के लिए डिजाइन किया गया था। वे प्रोटोकॉल सूचनाएँ, विशेष रूप से पासवर्ड, सादे संदर्भ में, उन्हें पैकेट विश्लेषण के लिए अवरोधन और प्रकटीकरण के लिए अतिसंवेदनशील प्रदान करते हैं। SSH द्वारा उपयोग किए गए एन्क्रिप्शन का उद्देश्य एक असुरक्षित नेटवर्क पर डेटा की गोपनीयता और अखंडता प्रदान करना है, जैसे कि इंटरनेट, हालांकि एडवर्ड स्नोडेन द्वारा लीक की गई फाइल्स संकेत देती हैं कि राष्ट्रीय सुरक्षा एजेंसी कभी–कभी SSH को डिक्रिप्ट कर सकती है, जिससे वे SSH सत्रों की सामग्री को पढ़ने की अनुमति दे सकते हैं।

SSH दूरस्थ कम्प्यूटर को प्रमाणित करने के लिए सार्वजनिक कुंजी क्रिप्टोग्राफी का उपयोग करता है और यदि आवश्यक हो, तो उपयोगकर्ता को प्रमाणित करने की अनुमति देता है। SSH का उपयोग करने की कई विधियाँ हैं। एक नेटवर्क कनेक्शन को एन्क्रिप्ट करने के लिए स्वचालित रूप से उत्पन्न सार्वजनिक–निजी कुंजी जोड़े का उपयोग करना है, और फिर लॉग ऑन करने के लिए पासवर्ड प्रमाणीकरण का उपयोग करें।

एक अन्य प्रमाणिक रूप से निर्मित सार्वजनिक–व्यक्तिगत कुंजी के युग्म का उपयोग प्रमाणीकरण करने के लिए होता है, जिससे उपयोगकर्ता या प्रोग्राम को पासवर्ड निर्दिष्ट किए बिना लॉग इन करने की अनुमति मिलती है। इस परिदृश्य में, कोई भी अलग–अलग कुंजी (सार्वजनिक और व्यक्तिगत) का एक सुमेलन युग्म का उत्पादन कर सकता है। सार्वजनिक कुंजी को उन सभी कम्प्यूटर्स पर रखा जाता है, जिन्हें सुमेलित व्यक्तिगत कुंजी के स्वामी तक पहुँच की अनुमति देनी चाहिए (स्वामी व्यक्तिगत कुंजी को गुप्त रखता है)। जबकि प्रमाणीकरण व्यक्तिगत कुंजी पर आधारित है, प्रमाणीकरण के दौरान कुंजी को कभी भी नेटवर्क के माध्यम से स्थानांतरित नहीं किया जाता है। SSH केवल इस बात की पुष्टि करता है कि क्या सार्वजनिक कुंजी की पेशकश करने वाला व्यक्ति भी सुमेलित करने वाली व्यक्तिगत कुंजी का मालिक है। SSH के सभी संस्करणों में, अज्ञात सार्वजनिक कुंजियों को सत्यापित करना महत्वपूर्ण है, अर्थात् सार्वजनिक कुंजियों को मान्य मानने से पहले उन्हें पहचान के साथ संबद्ध करना। सत्यापन के बिना किसी हमलावर की सार्वजनिक कुंजी स्वीकार करना एक वैध उपयोगकर्ता के रूप में अनधिकृत हमलावर को अधिकृत करेगा।

SSH की मुख्य विशेषताएं निम्न प्रकार हैं:

- एसएसएच एक नेटवर्क प्रोटोकॉल है जो TCP/IP परत के ऊपर चलता है। यह TELNET को बदलने के लिए डिजाइन किया गया है जो दूरस्थ लॉगऑन सुविधा का असुरक्षित साधन प्रदान करता है।
- SSH एक सुरक्षित क्लाइंट/सर्वर संचार प्रदान करता है और इसका उपयोग फाइल स्थानांतरण और ई–मेल जैसे कार्यों के लिए किया जा सकता है। SSH2 एक प्रचलित प्रोटोकॉल है जो पूर्व संस्करण SSH1 पर बेहतर नेटवर्क संचार सुरक्षा प्रदान करता है।

SSH को निम्न प्रकार तीन उप–प्रोटोकॉल के रूप में आयोजित किया जाता है:

1. ट्रांसपोर्ट लेयर प्रोटोकॉल: SSH प्रोटोकॉल का यह भाग डेटा गोपनीयता, सर्वर (होस्ट) प्रमाणीकरण और डेटा अखंडता प्रदान करता है। यह वैकल्पिक रूप से डेटा संपीड़न भी प्रदान कर सकता है।

- **सर्वर प्रमाणीकरणः** होस्ट कुंजी सार्वजनिक/व्यक्तिगत कुंजी की तरह असममित हैं। एक क्लाइंट के लिए अपनी पहचान साबित करने के लिए एक सार्वजनिक कुंजी का उपयोग करता है। क्लाइंट सत्यापित करता है कि सर्वर से एक ज्ञात होस्ट है जो इसे बनाए रखता है। एक बार सर्वर प्रमाणित हो जाने के बाद, सत्र कुंजी उत्पन्न होती है।
- **सत्र कुंजी स्थापनाः** प्रमाणीकरण के बाद, सर्वर और ग्राहक सिफर का उपयोग करने के लिए सहमत होते हैं। क्लाइंट और सर्वर दोनों द्वारा सत्र कुंजियाँ उत्पन्न की जाती हैं। उपयोगकर्ता प्रमाणीकरण से पहले सत्र कुंजी उत्पन्न की जाती है ताकि उपयोगकर्ता नाम और पासवर्ड एन्क्रिप्ट किए जा सकें। इन कुंजियों को आम तौर पर सत्र के दौरान नियमित अंतराल (जैसे, प्रत्येक घंटे) पर प्रतिस्थापित किया जाता है और उपयोग के तुरंत बाद नष्ट कर दिया जाता है।
- **डेटा अखंडताः** SSH डेटा अखंडता परीक्षण के लिए संदेश प्रमाणीकरण कोड (MAC) एल्गोरिथ्म का उपयोग करता है। यह SSH1 द्वारा उपयोग किए जाने वाले 32 बिट CRC पर एक सुधार है।

2. उपयोगकर्ता प्रमाणीकरण प्रोटोकॉल: SSH का यह भाग उपयोगकर्ता को सर्वर पर प्रमाणित करता है। सर्वर सत्यापित करता है कि पहुँच केवल इच्छित उपयोगकर्ताओं को दिया गया है। वर्तमान में कई प्रमाणीकरण विधियों का उपयोग किया जाता है जैसे, टाइप किए गए पासवर्ड, केर्बरोस (Kerberos), सार्वजनिक–कुंजी प्रमाणीकरण, आदि।

3. कनेक्शन प्रोटोकॉलः यह एक अंतर्निहित SSH कनेक्शन पर कई तार्किक चैनल प्रदान करता है।

SSH सेवाएँः

SSH तीन मुख्य सेवाएं प्रदान करता है जो कई सुरक्षित समाधानों के प्रावधान को सक्षम करता है। इन सेवाओं को संक्षेप में निम्नानुसार वर्णित किया गया है:

सिक्योर कमांड–शेल (रिमोट लॉगऑन): यह उपयोगकर्ता को फाइल्स को संपादित करने, निर्देशिकाओं की सामग्री को देखने और संयोजित डिवाइस पर एप्लिकेशन एक्सेस करने की अनुमति देता है। सिस्टम प्रशासक सेवाओं और प्रक्रियाओं को दूरस्थ रूप से प्रारंभ/देख/रोक सकते हैं, उपयोगकर्ता खाते बना सकते हैं, और फाइल/निर्देशिका अनुमतियों को बदल सकते हैं। मशीन के कमांड प्रॉम्प्ट पर संभव होने वाले सभी कार्यों को अब रिमोट मशीन से सुरक्षित रिमोट लॉगऑन का उपयोग करके सुरक्षित रूप से किया जा सकता है।

सुरक्षित फाइल स्थानांतरण: SSH फाइल स्थानांतरण प्रोटोकॉल (SFTP) सुरक्षित फाइल स्थानांतरण के लिए SSH–2 के विस्तार के रूप में डिजाइन किया गया है। संक्षेप में, यह फाइल स्थानांतरण को संभालने के लिए सुरक्षित शेल प्रोटोकॉल पर स्तरित एक पृथक प्रोटोकॉल है। SFTP उपयोगकर्ता नाम/पासवर्ड और स्थानांतरित किए जा रहे फाइल डेटा दोनों को एन्क्रिप्ट करता है। यह सिक्योर शेल सर्वर के समान पोर्ट का उपयोग करता है, यानी सिस्टम पोर्ट नंबर 22।

पोर्ट फॉरवर्डिंग (टनलिंग): यह असुरक्षित TCP/IP आधारित अनुप्रयोगों से डेटा को सुरक्षित रखने की अनुमति देता है। पोर्ट फॉरवर्डिंग स्थापित होने के बाद, सुरक्षित शैल एक प्रोग्राम (आमतौर पर क्लाइंट) से ट्रैफिक को पुनः जोड़ता है और एन्क्रिप्टेड टनल के पार दूसरी ओर (आमतौर पर एक सर्वर) प्रोग्राम में भेजता है।

एकाधिक अनुप्रयोग एक एकल मल्टीप्लेक्स सुरक्षित चैनल पर डेटा संचारित कर सकते हैं, जिससे फायरवॉल या राउटर पर कई पोर्ट खोलने की आवश्यकता समाप्त हो सकती है।

उपयोगः

SSH का उपयोग आमतौर पर एक दूरस्थ मशीन में लॉग इन करने और कमांड निष्पादित करने के लिए किया जाता है, लेकिन यह TCP पोर्ट और X11 कनेक्शन को अग्रेषित करने, सुरंग बनाने का भी समर्थन करता है। यह संबद्ध SSH फाइल स्थानांतरण (SFTP) या सुरक्षित प्रतिलिपि (SCP) प्रोटोकॉल का उपयोग करके फाइल्स स्थानांतरित कर सकता है। SSH क्लाइंट–सर्वर मॉडल का उपयोग करता है। SSH सर्वर से संपर्क करने के लिए मानक TCP पोर्ट 22 को सौंपा गया है।

एक SSH क्लाइंट प्रोग्राम का उपयोग आमतौर पर SSH डोमेन से रिमोट कनेक्शन स्वीकार करने के लिए कनेक्शन स्थापित करने हेतु किया जाता है। दोनों आमतौर पर अधिकांश आधुनिक ऑपरेटिंग सिस्टम पर मौजूद हैं, जिसमें macOS, लिनक्स के अधिकांश वितरण, OpenBSD, FreeBSD, NetBSD, Solaris और OpenVMS सम्मिलित हैं। विशेष रूप से, 1709 से पहले के विंडोज के संस्करणों में डिफॉल्ट रूप से SSH सम्मिलित नहीं है।

इंटरनेट पर सीधे क्लाउड आधारित वर्चुअल मशीन को उजागर करने के सुरक्षा मुद्दों से बचने के लिए, कनेक्टिविटी समस्याओं को हल करने के लिए क्लाउड कंप्यूटिंग में SSH महत्वपूर्ण है। एक SSH सुरंग एक फायरवॉल से एक आभासी मशीन के माध्यम से, इंटरनेट पर एक सुरक्षित मार्ग प्रदान कर सकती है।

10.6 लाभ और सीमायें:

ट्रांस्पोर्ट परत पर संचार सुरक्षा को नियोजित करने के लाभ और सीमाएँ निम्न प्रकार हैं:

लाभः

- ट्रांसपोर्ट परत सिक्योरिटी अनुप्रयोगों के लिए पारदर्शी है।
- सर्वर प्रमाणित है।
- एप्लिकेशन परत हेडर छिपे हुए हैं।
- यह परत 3 (IPsec) में सुरक्षा तंत्र की तुलना में अधिक बारीक है क्योंकि यह ट्रांसपोर्ट कनेक्शन स्तर पर काम करता है।

सीमाएंः

- केवल TCP आधारित अनुप्रयोगों के लिए लागू (UDP नहीं)।
- TCP/IP हेडर स्पष्ट हैं।
- क्लाइंट और सर्वर के मध्य सीधे संवाद के लिए उपयुक्त है। सर्वर की श्रृंखला (जैसे ईमेल) का उपयोग करके सुरक्षित अनुप्रयोगों के लिए पूरा नहीं करता है।
- प्रमाणीकरण वैकल्पिक होने के कारण क्लाइंट को SSL नॉन–रेगुलेशन प्रदान नहीं करता है।
- यदि आवश्यक हो, तो क्लाइंट प्रमाणीकरण को SSL से ऊपर लागू किया जाना चाहिए।

ट्रांसपोर्ट परत का सार संक्षेपः

पिछले एक दशक में इंटरनेट पर बड़ी संख्या में वेब एप्लिकेशन सामने आए हैं। कई ई–गवर्नेंस और ई–कॉमर्स पोर्टल ऑनलाइन आ गए हैं। इन एप्लिकेशन को सर्वर और क्लाइंट के मध्य उस सत्र की आवश्यकता होती है जो सत्रों की गोपनीयता, प्रमाणीकरण और अखंडता प्रदान करने के लिए सुरक्षित है।

उपयोगकर्ता के सत्र के दौरान संभावित हमले को कम करने का एक तरीका सुरक्षित संचार प्रोटोकॉल का उपयोग करना है। इस तरह के दो संचार प्रोटोकॉल, सिक्योर सॉकेट्स लेयर (SSL) और ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) की इस अध्याय में चर्चा की गई है। ये दोनों प्रोटोकॉल ट्रांसपोर्ट लेयर पर काम करते हैं।

TELNET को बदलने के लिए डिजाइन किया गया एक अन्य ट्रांसपोर्ट लेयर प्रोटोकॉल, सिक्योर शेल (SSH), रिमोट लॉगऑन सुविधा का सुरक्षित साधन प्रदान करता है। यह विभिन्न सेवाओं जैसे सिक्योर कमांड शेल और SFTP प्रदान करने में सक्षम है।

ट्रांसपोर्ट लेयर सिक्योरिटी के कई लाभ हैं। हालाँकि, इन परत पर डिजाइन किए गए सुरक्षा प्रोटोकॉल का उपयोग केवल TCP के साथ किया जा सकता है। वे UDP का उपयोग करके लागू संचार के लिए सुरक्षा प्रदान नहीं करते हैं।

अभ्यास

1. ट्रांस्पोर्ट लेयर (परिवहन परत) सुरक्षा की आवश्यकता क्यों होती है?
2. सिक्योर सॉकेट लेयर (सुरक्षित सॉकेट परत) पर संक्षिप्त टिप्पणी लिखिए।
3. TLS प्रोटोकॉल (संदेशाचार) क्या है?
4. सिक्योर (सुरक्षित) ब्राउजिंग से क्या समझते हैं?
5. सिक्योर शेल प्रोटोकॉल (सुरक्षित शेल संदेशाचार) को विस्तार से समझाइए।
6. ट्रांस्पोर्ट लेयर के लाभ और सीमाओं को बताइए।

अध्याय – 11

नेटवर्क लेयर
(जालक्रम परत)

OSI मॉडल में लेयर –3 को नेटवर्क लेयर या नेटवर्क परत कहा जाता है। नेटवर्क परत होस्ट और नेटवर्क एड्रेसिंग, सब–नेटवर्क और इंटरनेटवर्किंग के प्रबंधन से संबंधित विकल्पों का प्रबंधन करता है।

नेटवर्क परत पैकेट को एक सबनेट के अंदर या बाहर स्रोत से गंतव्य तक ले जाने की जिम्मेदारी लेता है। दो अलग–अलग सबनेट में अलग–अलग एड्रेसिंग स्कीम या गैर–संगत एड्रेसिंग प्रकार हो सकते हैं। प्रोटोकॉल के साथ भी, दो अलग–अलग सबनेट अलग–अलग प्रोटोकॉल पर काम कर सकते हैं जो एक दूसरे के साथ संगत नहीं हैं। नेटवर्क लेयर में पैकेट को स्रोत से गंतव्य तक भेजने की जिम्मेदारी होती है, विभिन्न एड्रेसिंग स्कीम और प्रोटोकॉल की मैपिंग होती है।

नेटवर्क परत सुरक्षा नियंत्रणों का उपयोग संचार को सुरक्षित करने के लिए अक्सर किया जाता है, विशेष रूप से इंटरनेट जैसे साझा नेटवर्क पर क्योंकि वे कई अनुप्रयोगों के लिए एक बार में उन्हें संशोधित किए बिना सुरक्षा प्रदान कर सकते हैं।

पूर्व में, हमने चर्चा की कि कई वास्तविक समय सुरक्षा प्रोटोकॉल नेटवर्क सुरक्षा के लिए विकसित हुए हैं, जो गोपनीयता, मूल प्रमाणीकरण, संदेश अखंडता, और गैर–अस्वीकरण जैसे सुरक्षा के बुनियादी सिद्धांतों को सुनिश्चित करते हैं।

इनमें से अधिकांश प्रोटोकॉल मानक इंटरनेट प्रोटोकॉल में अंतर्निहित सुरक्षा की कमी की भरपाई के लिए, OSI प्रोटोकॉल स्टैक की उच्च परतों पर केंद्रित रहे। हालांकि मूल्यवान, इन विधियों को किसी भी एप्लिकेशन के साथ उपयोग के लिए आसानी से सामान्यीकृत नहीं किया जा सकता है। उदाहरण के लिए, SSL विशेष रूप से HTTP या FTP जैसे अनुप्रयोगों को सुरक्षित करने के लिए विकसित किया गया है। लेकिन कई अन्य एप्लिकेशन भी हैं जिन्हें सुरक्षित संचार की आवश्यकता है।

इस आवश्यकता ने IP परत पर एक सुरक्षा समाधान विकसित करने के लिए वृद्धि दी ताकि सभी उच्च–परत प्रोटोकॉल इसका लाभ उठा सकें। 1992 में, इंटरनेट इंजीनियरिंग टास्क फोर्स (IETF) ने एक मानक IPsec को परिभाषित करना शुरू किया।

इस अध्याय में, हम चर्चा करेंगे कि प्रोटोकॉल IPsec के इस बहुत लोकप्रिय सेट का उपयोग करके नेटवर्क परत पर सुरक्षा कैसे प्राप्त की जाती है।

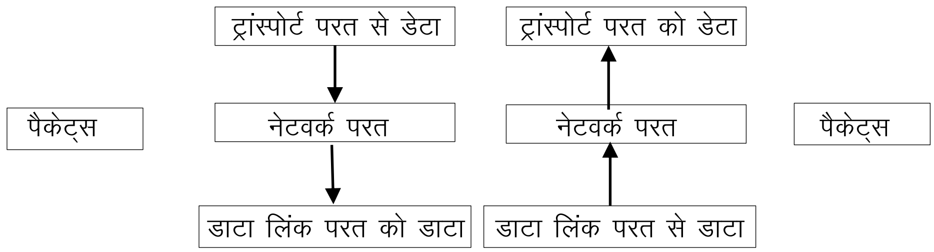
नेटवर्क परत सबनेट के संचालन को नियंत्रित करता है। इस परत का मुख्य उद्देश्य स्रोत से गंतव्य तक कई लिंक (नेटवर्क) तक पहुंचाना है। यदि दो कम्प्यूटर (सिस्टम) एक ही लिंक पर जुड़े हुए हैं, तो नेटवर्क परत की कोई आवश्यकता नहीं है। यह विभिन्न चैनलों के माध्यम से दूसरे छोर तक सिग्नल को रूट करता है और नेटवर्क नियंत्रक के रूप में कार्य करता है।

यह बाहर जाने वाले संदेशों को पैकेट में विभाजित करता है और आने वाले पैकेट्स को उच्च स्तरों के लिए संदेशों में इकट्ठा करता है।

प्रसारण नेटवर्क में, रूटिंग की समस्या सरल है, इसलिए नेटवर्क परत अक्सर पतली या न के बराबर होती है।

नेटवर्क परत के कार्यः

1. यह तार्किक नेटवर्क पते का भौतिक पते में अनुवाद करता है। सर्किट, संदेश या पैकेट स्विचिंग से संबंधित।
2. राउटर और गेटवे नेटवर्क परत में काम करते हैं। पैकेट को अंतिम गंतव्य तक पहुँचाने के लिए नेटवर्क परत द्वारा तंत्र प्रदान किया जाता है।
3. कनेक्शन सेवाएं नेटवर्क परत प्रवाह नियंत्रण, नेटवर्क परत त्रुटि नियंत्रण और पैकेट अनुक्रम नियंत्रण सहित प्रदान की जाती हैं।
4. बड़े पैकेट को छोटे पैकेट में तोड़ता है।



(चित्र क्र0 11.1)

नेटवर्क परत के साथ डिजाइन के मुद्दे:

- एक प्रमुख डिजाइन मुद्दा यह निर्धारित करता है कि पैकेट को स्रोत से गंतव्य तक कैसे पहुँचाया जाए। रूट स्थिर तालिकाओं पर आधारित हो सकते हैं जो नेटवर्क में वायर्ड होते हैं और शायद ही कभी बदले जाते हैं। वे अत्यधिक गतिशील भी हो सकते हैं, प्रत्येक पैकेट के लिए नए सिरे से निर्धारित किया जा रहा है, ताकि वर्तमान नेटवर्क लोड को प्रतिबिंबित किया जा सके।
- यदि एक ही समय में बहुत सारे पैकेट सबनेट में मौजूद हैं, तो वे एक दूसरे के रास्ते में आ जाएंगे, जिससे कठिनाई उत्पन्न होंगी। इस तरह की भीड़ का नियंत्रण भी नेटवर्क परत के अंतर्गत आता है।
- इसके अतिरिक्त, प्रदान की गई सेवा की गुणवत्ता (देरी, संचारित समय, घबराना, आदि) भी एक नेटवर्क परत समस्या है।
- जब एक पैकेट को अपने गंतव्य तक पहुँचने के लिए एक नेटवर्क से दूसरे नेटवर्क पर जाना पड़ता है, तो कई समस्याएं उत्पन्न हो सकती हैं जैसे:
  - दूसरे नेटवर्क द्वारा उपयोग की जाने वाली एड्रेसिंग पहले वाले से अलग हो सकती है।
  - दूसरा व्यक्ति पैकेट को बिल्कुल स्वीकार नहीं कर सकता क्योंकि यह बहुत बड़ा है।
  - प्रोटोकॉल भिन्न हो सकते हैं, और इसी तरह।
- यह नेटवर्क परत पर निर्भर है कि इन सभी समस्याओं को दूर करने के लिए विषम नेटवर्क को आपस में जोड़ा जाए।

नेटवर्क परत विशेषताएं:

इसकी मानक कार्यक्षमता के साथ, लेयर 3 विभिन्न विशेषताएं प्रदान कर सकता है:

- सेवा प्रबंधन की गुणवत्ता
- लोड संतुलन और लिंक प्रबंधन
- सुरक्षा
- विभिन्न योजनाओं के साथ विभिन्न प्रोटोकॉल और सबनेट का परस्पर संबंध।
- भौतिक नेटवर्क डिजाइन पर विभिन्न तार्किक नेटवर्क डिजाइन।
- L3 VPN और सुरंगों का उपयोग समर्पित कनेक्टिविटी को समाप्त करने के लिए किया जा सकता है।

इंटरनेट प्रोटोकॉल को व्यापक रूप से सम्मानित किया जाता है और नेटवर्क परत प्रोटोकॉल को तैनात किया जाता है जो इंटरनेट पर एंड–से–एंड डिवाइसेस का संचार करने में मदद करता है। यह दो प्रकार में आता है। IPv4 जिसने दशकों तक दुनिया पर राज किया है लेकिन अब पता स्थान से बाहर चल रहा है। IPv6 को IPv4 को बदलने के लिए बनाया गया है और उम्मीद है कि IPv4 की सीमाओं को भी कम किया जाएगा।

नेटवर्क लेयर प्रोटोकॉलः

नेटवर्क के प्रत्येक कम्प्यूटर का एक IP पता होता है जिसके द्वारा इसे विशिष्ट रूप से पहचाना और संबोधित किया जा सकता है। एक IP एड्रेस लेयर –3 (नेटवर्क लेयर) लॉजिकल एड्रेस है। यह पता हर बार कम्प्यूटर के पुनः आरंभ होने पर बदल सकता है। एक कम्प्यूटर में एक समय में एक IP और कुछ अलग समय में एक पृथक IP हो सकता है।

1. एड्रेस रिजॉल्यूशन प्रोटोकॉल (ARP):

संचार करते समय, एक होस्ट को गंतव्य मशीन के लेयर –2 (MAC) पते की आवश्यकता होती है जो उसी प्रसारण डोमेन या नेटवर्क से संबंधित है। एक MAC पते को मशीन के नेटवर्क इंटरफेस कार्ड (NIC) में भौतिक रूप से बर्न किया जाता है और यह कभी नहीं बदलता है।

दूसरी ओर, सार्वजनिक डोमेन पर IP पता शायद ही कभी बदला जाता है। यदि कुछ गलती के मामले में NIC को बदल दिया जाता है, तो MAC पता भी बदल जाता है। इस तरह, लेयर –2 संचार के लिए, दोनों के बीच एक मानचित्रण की आवश्यकता होती है।

प्रसारण डोमेन पर दूरस्थ होस्ट का MAC पता जानने के लिए, संचार शुरू करने के इच्छुक कम्प्यूटर ARP प्रसारण संदेश भेजते हुए पूछते हैं, 'यह IP पता किसके पास है?' क्योंकि यह एक प्रसारण है, नेटवर्क सेगमेंट पर सभी होस्ट (प्रसारण डोमेन)) इस पैकेट को प्राप्त करें और इसे संसाधित करें। ARP पैकेट में गंतव्य होस्ट का IP पता होता है, जिसे होस्ट बात करने के लिए भेजता है। जब कोई होस्ट ARP पैकेट प्राप्त करता है, तो वह अपने MAC पते के साथ वापस आ जाता है।

एक बार होस्ट को गंतव्य MAC पता मिल जाता है, यह लेयर –2 लिंक प्रोटोकॉल का उपयोग करके दूरस्थ होस्ट के साथ संवाद कर सकता है। यह MAC से IP मैपिंग होस्ट्स को भेजने और प्राप्त करने दोनों के ARP कैश में सहेजा जाता है। अगली बार, अगर उन्हें संवाद करने की आवश्यकता होती है, तो वे सीधे अपने संबंधित ARP कैश का उल्लेख कर सकते हैं।

व्युत्क्रम ARP एक ऐसा तंत्र है जहाँ होस्ट दूरस्थ होस्ट के MAC पते को जानता है लेकिन संचार करने के लिए IP पते को जानना आवश्यक है।

2. इंटरनेट कंट्रोल मैसेज प्रोटोकॉल (ICMP):

ICMP नेटवर्क डायग्नोस्टिक और एरर रिपोर्टिंग प्रोटोकॉल है। ICMP, IP प्रोटोकॉल सूट के अंतर्गत आता है और वाहक प्रोटोकॉल के रूप में IP का उपयोग करता है। ICMP पैकेट के निर्माण के बाद, इसे IP पैकेट में एन्क्रिप्ट किया जाता है। क्योंकि IP स्वयं एक सर्वश्रेष्ठ प्रयास गैर–विश्वसनीय प्रोटोकॉल है, इसलिए ICMP है।

नेटवर्क के बारे में कोई भी प्रतिक्रिया मूल होस्ट को वापस भेज दी जाती है। यदि नेटवर्क में कुछ त्रुटि होती है, तो उसे ICMP के माध्यम से सूचित किया जाता है। ICMP में दर्जनों नैदानिक और त्रुटि रिपोर्टिंग संदेश सम्मिलित हैं।

ICMP-echo और ICMP–echo–reply सबसे आम तौर पर उपयोग किए जाने वाले ICMP संदेश हैं जो एंड–से–एंड होस्ट्स के पहुँच का परीक्षण करते हैं। जब कोई होस्ट ICMP–echo रिक्वेस्ट प्राप्त करता है, तो वह ICMP-echo-response को वापस भेजने के लिए बाध्य होता है। यदि पारगमन नेटवर्क में कोई समस्या है, तो ICMP उस समस्या की रिपोर्ट करेगा।

3. इंटरनेट प्रोटोकॉल संस्करण 4 (IPv4):

IPv4 32–बिट एड्रेसिंग स्कीम है जिसे TCP/IP होस्ट एड्रेसिंग मैकेनिज्म के रूप में उपयोग किया जाता है। IP एड्रेसिंग TCP/IP नेटवर्क पर हर मेजबान को विशिष्ट पहचान योग्य बनाता है।

IPv4 पदानुक्रमित पता योजना प्रदान करता है जो इसे नेटवर्क को उप–नेटवर्क में विभाजित करने में सक्षम बनाता है, प्रत्येक मेजबान की अच्छी तरह से परिभाषित संख्या के साथ। IP पते कई श्रेणियों में विभाजित हैं:

क्लास ए – यह नेटवर्क एड्रेस के लिए प्रथम ऑक्टेट और होस्ट एड्रेसिंग के लिए अंतिम तीन ऑक्टेट का उपयोग करता है।

क्लास बी – यह नेटवर्क पते के लिए पहले दो ऑक्टेट्स का उपयोग करता है और अंतिम दो होस्ट एड्रेसिंग के लिए।

क्लास सी – यह नेटवर्क एड्रेस के लिए प्रथम तीन ऑक्टेट्स का उपयोग करता है और होस्ट एड्रेसिंग के लिए अंतिम होता है।
क्लास डी – यह तीन से ऊपर के लिए पदानुक्रमित संरचना के विपरीत फ्लैट IP एड्रेसिंग योजना प्रदान करता है।
क्लास ई – यह प्रयोग के रूप में उपयोग किया जाता है।

IPv4 में व्यक्तिगत पते (इंटरनेट पर राउटेबल नहीं) और सार्वजनिक पतों (ISP द्वारा प्रदान किए गए और इंटरनेट पर राउटेबल हैं) के रूप में उपयोग करने के लिए अच्छी तरह से परिभाषित स्थान हैं। हालांकि IP विश्वसनीय नहीं है। यह 'सर्वश्रेष्ठ–प्रयास–वितरण' तंत्र प्रदान करता है।

4. इंटरनेट प्रोटोकॉल संस्करण 6 (IPv6):

IPv4 पतों की कमियों ने अगली पीढ़ी के इंटरनेट प्रोटोकॉल संस्करण 6 को जनित किया। IPv6 ने अपने नोड्स को 128–बिट चौड़े पते के साथ संबोधित किया है, जो भविष्य के लिए पूरे ग्रह या उससे परे उपयोग किए जाने के लिए बहुत अधिक स्थान प्रदान करता है।

IPv6 ने Anycast को संबोधित किया है लेकिन प्रसारण की अवधारणा को हटा दिया है। IPv6 उपकरणों को IPv6 पते को स्व–प्राप्त करने और उस सबनेट के भीतर संचार करने में सक्षम बनाता है। यह ऑटो–कॉन्फिगरेशन डायनामिक होस्ट कॉन्फिगरेशन प्रोटोकॉल (Dynamic Host Configuration Protocol - DHCP) सर्वर की निर्भरता को दूर करता है। इस तरह, भले ही उस सबनेट पर DHCP सर्वर डाउन हो, होस्ट एक–दूसरे के साथ संवाद कर सकते हैं।

IPv6, IPv6 गतिशीलता की नई सुविधा प्रदान करता है। मोबाइल IPv6 सुसज्जित मशीनें अपने IP पते को बदलने की आवश्यकता के बिना घूम सकती हैं। IPv6 अभी भी संक्रमण के चरण में है और आने वाले वर्षों में IPv4 को पूरी तरह से बदलने की उम्मीद है। वर्तमान में, कुछ नेटवर्क हैं जो IPv6 पर चल रहे हैं। IPv6 सक्षम नेटवर्क के लिए कुछ संक्रमण तंत्र उपलब्ध हैं जो IPv4 पर विभिन्न नेटवर्क पर आसानी से बोल और घूम सकते हैं। ये हैं:

- दोहरी स्टैक कार्यान्वयन
- टनेलिंग
- NAT-PT

11.1 नेटवर्क लेयर (जालक्रम परत) में सुरक्षा:

नेटवर्क सुरक्षा प्रदान करने के लिए विकसित की गई किसी भी योजना को प्रोटोकॉल स्टैक में कुछ परत पर लागू करने की आवश्यकता है जैसा कि नीचे तालिका में दिखाया गया है:

परत	संचार प्रोटोकॉल	सुरक्षा प्रोटोकॉल
एप्लीकेशन परत	HTTP FTP SMTP	PGP. S/MIME, HTTPS
ट्रांस्पोर्ट परत	TCP /UDP	SSL, TLS, SSH
नेटवर्क परत	IP	IPsec

नेटवर्क परत पर सुरक्षा सुनिश्चित करने के लिए विकसित लोकप्रिय ढांचा इंटरनेट प्रोटोकॉल सिक्योरिटी (IPsec) है।

IPsec की विशेषताएं:

- IPsec केवल ट्रांसपोर्ट प्रोटोकॉल के रूप में TCP के साथ काम करने के लिए डिजाइन नहीं किया गया है। यह UDP के साथ–साथ IP के ऊपर किसी भी अन्य प्रोटोकॉल जैसे ICMP, OSPF आदि के साथ काम करता है।
- IPsec उच्च परत हेडर सहित IP परत को प्रस्तुत पूरे पैकेट की सुरक्षा करता है।
- चूंकि उच्च स्तर के हेडर छिपे होते हैं जो पोर्ट नंबर ले जाते हैं, ट्रैफिक विश्लेषण अधिक कठिन होता है।

- IPsec एक नेटवर्क इकाई से दूसरी नेटवर्क इकाई के लिए काम करता है, आवेदन प्रक्रिया से आवेदन प्रक्रिया तक नहीं। इसलिए, व्यक्तिगत उपयोगकर्ता कम्प्यूटर/अनुप्रयोगों में परिवर्तन की आवश्यकता के बिना सुरक्षा को अपनाया जा सकता है।
- व्यापक रूप से नेटवर्क संस्थाओं के मध्य सुरक्षित संचार प्रदान करने के लिए उपयोग किया जाता है, IPsec होस्ट–से–होस्ट सुरक्षा भी प्रदान कर सकता है।
- IPsec का सबसे आम उपयोग दो स्थानों (गेटवे–से–गेटवे) या एक दूरस्थ उपयोगकर्ता और एक एंटरप्राइज नेटवर्क (होस्ट–से–गेटवे) के मध्य एक वर्चुअल प्राइवेट नेटवर्क (VPN) प्रदान करना है।

सुरक्षा कार्यः

IPsec द्वारा प्रदान किए गए महत्वपूर्ण सुरक्षा कार्य निम्न प्रकार हैंः

1. गोपनीयताः
   - संदेशों को एन्क्रिप्ट करने के लिए नोड्स का संचार करने में सक्षम बनाता है।
   - तृतीय पक्षों द्वारा उल्लिखित को रोकना।
2. मूल प्रमाणीकरण और डेटा अखंडता।
   - यह आश्वासन देता है कि प्राप्त पैकेट को वास्तव में पैकेट हेडर के स्रोत के रूप में पहचाने गये पक्ष द्वारा प्रेषित किया गया था।
   - पुष्टि करता है कि पैकेट को बदल दिया गया है या नहीं।

मुख्य प्रबंधन।
- कुंजियों के सुरक्षित आदान–प्रदान की अनुमति देता है।
- कुछ प्रकार के सुरक्षा हमलों, जैसे कि रिप्ले हमलों के खिलाफ सुरक्षा।

वर्चुअल प्राइवेट नेटवर्कः

आदर्श रूप से, कोई भी संस्था सुरक्षा सुनिश्चित करने के लिए संचार के लिए अपना निजी नेटवर्क चाहेगी। हालांकि, भौगोलिक रूप से छितरी हुई जगह पर इस तरह के निजी नेटवर्क को स्थापित करना और बनाए रखना बहुत महंगा हो सकता है। इसके लिए संचार लिंक, राउटर, DNS आदि के जटिल बुनियादी ढांचे का प्रबंधन करना होगा।

IPsec ऐसे संस्थानों के लिए वर्चुअल प्राइवेट नेटवर्क (VPN) को लागू करने के लिए एक आसान तंत्र प्रदान करता है। VPN तकनीक संस्था के अंतर–कार्यालय यातायात को सार्वजनिक इंटरनेट में प्रवेश करने से पहले ट्रैफिक को एन्क्रिप्ट करके और इसे अन्य ट्रैफिक से तार्किक रूप से अलग करके सार्वजनिक इंटरनेट पर भेजने की अनुमति देता है।

IP सुरक्षा प्रोटोकॉल, जिसे आमतौर पर IPsec के रूप में जाना जाता है, प्रोटोकॉल का एक सूट है जो नेटवर्क परत पर सुरक्षा प्रदान करता है। IPsec एक जटिल प्रोटोकॉल है – इसके लिए एक दर्जन से अधिक RFC में भाग दिए गए हैं।

पहले विचार करें कि नेटवर्क–परत गोपनीयता प्रदान करने का क्या अर्थ है। यदि सभी IP डेटाग्राम द्वारा लाये गए सभी डेटा एन्क्रिप्ट किए गए थे, तो नेटवर्क लेयर गोपनीयता प्रदान करेगा। जब भी कोई होस्ट डेटाग्राम भेजना चाहता है, तो वह नेटवर्क में शिपिंग से पहले डेटाग्राम के डेटा क्षेत्र को एन्क्रिप्ट कर देता है। सिद्धांत रूप में, एन्क्रिप्शन को सममित कुंजी एन्क्रिप्शन, सार्वजनिक कुंजी एन्क्रिप्शन या सत्र कुंजियों के साथ किया जा सकता है, जिन्हें सार्वजनिक कुंजी एन्क्रिप्शन का उपयोग करके बातचीत की जाती है। डेटा फील्ड एक TCP खंड, एक UDP खंड, एक ICMP संदेश, और इसी तरह हो सकता है। यदि इस तरह की नेटवर्क परत सेवा होती है, तो होस्ट द्वारा भेजे गए सभी डेटा जिसमें ई–मेल, वेब पेज, नियंत्रण संदेश और प्रबंधन संदेश शामिल हैं, किसी भी तीसरे पक्ष से छिपाए जाएंगे जो नेटवर्क का दोहन कर रहे थे।

गोपनीयता के अतिरिक्त, कोई भी नेटवर्क परत को स्रोत प्रमाणीकरण भी प्रदान कर सकता है। जब कोई गंतव्य होस्ट किसी विशेष IP स्रोत पते के साथ IP डेटाग्राम प्राप्त करता है, तो यह सुनिश्चित करता है कि IP डेटाग्राम वास्तव में उस IP स्रोत पते के साथ होस्ट द्वारा जनित किया गया है। इस तरह का एक सीरियस डेटाग्राम को IP पते को प्रमाणित करने से रोकता है।

IPsec प्रोटोकॉल सूट में दो प्रमुख प्रोटोकॉल हैं: ऑथेंटिकेशन हेडर (AH) प्रोटोकॉल और एनकैप्सुलेशन सिक्योरिटी पेलोड (ESP) प्रोटोकॉल। जब कोई स्रोत होस्ट सुरक्षित डेटाग्राम को किसी गंतव्य होस्ट को भेजता है, तो वह AH प्रोटोकॉल या ESP प्रोटोकॉल के साथ ऐसा करता है। AH प्रोटोकॉल स्रोत प्रमाणीकरण और डेटा अखंडता प्रदान करता है लेकिन गोपनीयता प्रदान नहीं करता है। ESP प्रोटोकॉल प्रमाणीकरण, डेटा पूर्णांक और गोपनीयता प्रदान करता है। अधिक सेवाएं प्रदान करना, ESP प्रोटोकॉल स्वाभाविक रूप से अधिक जटिल है और AH प्रोटोकॉल की तुलना में अधिक छिद्रण की आवश्यकता होती है।

AH और ESP प्रोटोकॉल दोनों में, सुरक्षित डेटाग्राम को स्रोत होस्ट से गंतव्य होस्ट पर भेजे जाने से पहले, स्रोत और नेटवर्क हैंडशेक होस्ट करते हैं और नेटवर्क–लेयर लॉजिकल कनेक्शन बनाते हैं। इस तार्किक चैनल को सुरक्षा संघ (SA) कहा जाता है।

एक SA को विशिष्ट रूप से तीन–टपल की सहमति से पहचाना जाता है:

- सुरक्षा प्रोटोकॉल (AH या ESP) पहचानकर्ता।
- सिम्प्लेक्स कनेक्शन के लिए स्रोत IP पता
- सुरक्षा पैरामीटर सूचकांक (SPI) नामक एक 32–बिट कनेक्शन पहचानकर्ता।

AH प्रोटोकॉल:

AH प्रोटोकॉल स्रोत होस्ट प्रमाणीकरण और डेटा अखंडता प्रदान करता है लेकिन गोपनीय नहीं। जब कोई विशेष स्रोत होस्ट किसी एक या अधिक डेटाग्राम को किसी विशेष गंतव्य पर भेजना चाहता है, तो वह सबसे पहले SA को गंतव्य के साथ स्थापित करता है। SA स्थापित होने के बाद, स्रोत सुरक्षित डाटाग्राम को गंतव्य होस्ट पर भेज सकता है। सुरक्षित डेटाग्राम में AH हेडर शामिल होता है, जो मूल आईपी डेटाग्राम डेटा और IP हेडर के मध्य रखा जाता है।

AH हेडर में कई क्षेत्र सम्मिलित हैं:

- अगला हेडर क्षेत्र, जिसमें एक साधारण डेटाग्राम के लिए प्रोटोकॉल फील्ड की भूमिका होती है।
- सुरक्षा पैरामीटर सूचकांक (SPI) क्षेत्र, एक वांछित 32–बिट मूल्य, जो गंतव्य IP पते और सुरक्षा प्रोटोकॉल के संयोजन में, विशिष्ट रूप से डाटाग्राम के लिए SA की पहचान करता है।
- अनुक्रम संख्या क्षेत्र, प्रत्येक डेटाग्राम के लिए अनुक्रम संख्या वाले 32–बिट क्षेत्र।
- प्रमाणीकरण डेटा क्षेत्र, एक चर–लंबाई क्षेत्र जिसमें इस डेटाग्राम के लिए हस्ताक्षरित संदेश डाइजेस्ट होता है।

जब गंतव्य होस्ट को AH हेडर के साथ IP डेटाग्राम प्राप्त होता है, तो यह SA को डेटाग्राम के लिए निर्धारित करता है और फिर प्रमाणीकरण डेटा क्षेत्र को संसाधित करके डेटाग्राम की अखंडता को प्रमाणित करता है।

ESP प्रोटोकॉल:

ESP प्रोटोकॉल नेटवर्क–परत गोपनीयता के साथ–साथ स्रोत होस्ट प्रमाणीकरण और डेटा अखंडता प्रदान करता है। यह सब एक स्रोत होस्ट के साथ आरंभ होता है एक गंतव्य होस्ट के साथ एक SA स्थापित करता है, तब स्रोत होस्ट सुरक्षित डेटाग्राम को गंतव्य होस्ट को भेज सकता है। IP डेटा के मूल क्षेत्र में मूल IP डेटाग्राम के आसपास एक सुरक्षित डेटाग्राम बनाया जाता है। IP डेटाग्राम के हेडर में प्रोटोकॉल क्षेत्र के लिए, मान 50 का उपयोग इंगित करने के लिए किया जाता है कि डेटाग्राम में ESP हेडर और ट्रेलर शामिल हैं। जब गंतव्य होस्ट IP डेटाग्राम प्राप्त करता है, तो यह प्रोटोकॉल फील्ड में 50 का ध्यान रखता है और ESP प्रोटोकॉल का उपयोग करके डेटाग्राम को प्रोसेस करता है।

SA और कुंजी प्रबंधन:

IPsec की सफल तैनाती के लिए, एक स्केलेबल और स्वचालित SA और कुंजी प्रबंधन योजना आवश्यक है। इन कार्यों के लिए कई प्रोटोकॉल परिभाषित किए गए हैं।

- इंटरनेट कुंजी एक्सचेंज (IKE) एल्गोरिथ्म IPsec के लिए डिफॉल्ट कुंजी प्रबंधन प्रोटोकॉल है।

- इंटरनेट सिक्योरिटी एसोसिएशन और कुंजी मैनेजमेंट प्रोटोकॉल (ISKMP) को स्थापित करने और खींचने की प्रक्रियाओं को परिभाषित करता है।

11.2 IPsec का आकलन:

IPsec, IP परत पर सुरक्षा प्रदान करने के लिए प्रोटोकॉल का एक फ्रेमवर्क/सूइट है। 1990 के दशक की शुरुआत में, कुछ संस्थानों द्वारा इंटरनेट का उपयोग किया गया था, ज्यादातर शैक्षणिक उद्देश्यों के लिए। लेकिन बाद के दशकों में, नेटवर्क के विस्तार और संचार और अन्य उद्देश्यों के लिए इसका उपयोग करने वाले कई संगठनों के कारण इंटरनेट का विकास तेजी से हुआ।

इंटरनेट की भारी वृद्धि के साथ, TCP/IP प्रोटोकॉल की अंतर्निहित सुरक्षा कमियों के साथ, एक ऐसी तकनीक की आवश्यकता महसूस की गई जो इंटरनेट पर नेटवर्क सुरक्षा प्रदान कर सके। 1994 में इंटरनेट आर्किटेक्चर बोर्ड (IAB) द्वारा 'इंटरनेट आर्किटेक्चर में सुरक्षा' नामक एक रिपोर्ट जारी की गई थी। इसने सुरक्षा तंत्र के प्रमुख क्षेत्रों की पहचान की।

IAB में अगली पीढ़ी के IPv6 में आवश्यक सुरक्षा सुविधाओं के रूप में प्रमाणीकरण और एन्क्रिप्शन सम्मिलित था। संयोग से, इन सुरक्षा क्षमताओं को इस तरह परिभाषित किया गया था कि उन्हें वर्तमान IPv4 और भविष्य IPv6 दोनों के साथ लागू किया जा सकता है।

सुरक्षा ढांचा, IPsec को 'टिप्पणियों के लिए अनुरोध' (RFCs) में परिभाषित किया गया है। कुछ RFC प्रोटोकॉल के कुछ भागों को निर्दिष्ट करते हैं, जबकि अन्य संपूर्ण रूप से समाधान को संबोधित करते हैं।

IPsec के अंदर संचालनः

IPsec सूइट को दो पृथक–पृथक संक्रिया माना जा सकता है, जब एक साथ प्रदर्शन किया जाता है, सुरक्षा सेवाओं का एक पूरा समूह प्रदान करता है। ये दो संक्रियायें हैं IPsec कम्युनिकेशन और इंटरनेट की एक्सचेंज।

IPsec संचारः

- यह आम तौर पर मानक IPsec कार्यक्षमता के साथ जुड़ा हुआ है। इसमें इनकैप्सुलेशन, एन्क्रिप्शन और IP डेटाग्राम के हैशिंग और सभी पैकेट प्रक्रियाओं को सम्मिलित करना शामिल है।
- यह संचार पक्षों के मध्य स्थापित सुरक्षा संघों के अनुसार संचार के प्रबंधन के लिए उत्तरदायी है।
- यह प्रमाणीकरण हैडर (AH) और एनकैप्सुलेटेड SP (ESP) जैसे सुरक्षा प्रोटोकॉल का उपयोग करता है।
- IPsec संचार कुंजी या उनके प्रबंधन के निर्माण में शामिल नहीं है।
- IPsec संचार संक्रिया को आमतौर पर IPsec कहा जाता है।

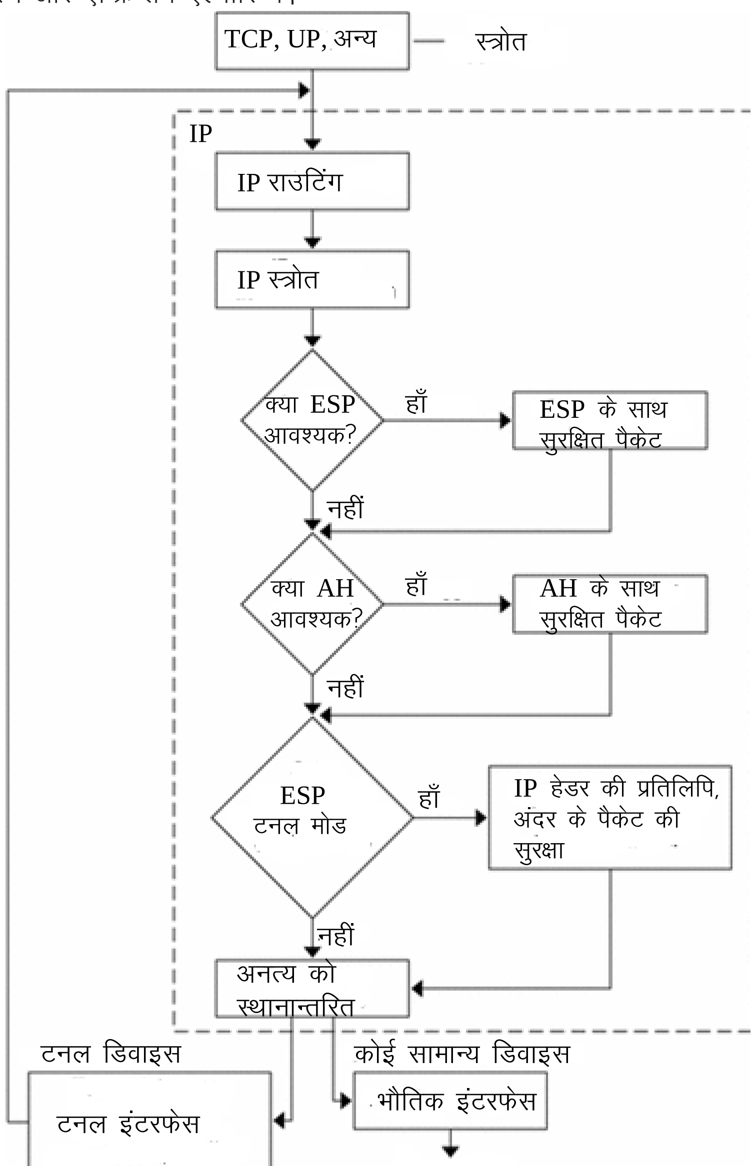
इंटरनेट कुंजी विनिमय (IKE):

- IKE, IPsec के लिए उपयोग किया जाने वाला स्वचालित कुंजी प्रबंधन प्रोटोकॉल है।
- तकनीकी रूप से, IPsec संचार के लिए मुख्य प्रबंधन आवश्यक नहीं है और कुंजी को मैन्युअल रूप से प्रबंधित किया जा सकता है। हालांकि, बड़े नेटवर्क के लिए मैन्युअल कुंजी प्रबंधन वांछनीय नहीं है।
- IKE, IPsec के लिए कुंजियों के निर्माण और कुंजी स्थापना प्रक्रिया के दौरान प्रमाणीकरण प्रदान करने के लिए उत्तरदायी है। हालाँकि, IPsec का उपयोग किसी अन्य प्रमुख प्रबंधन प्रोटोकॉल के लिए किया जा सकता है, IKE का उपयोग डिफॉल्ट रूप से किया जाता है।
- IKE दो प्रोटोकॉल (Oakley और SKEME) को परिभाषित करता है जिसका उपयोग पहले से ही परिभाषित कुंजी प्रबंधन ढांचे इंटरनेट सुरक्षा एसोसिएशन कुंजी प्रबंधन प्रोटोकॉल (ISAKMP) के साथ किया जाता है।

- ISAKMP, IPsec विशिष्ट नहीं है, लेकिन किसी भी प्रोटोकॉल के लिए SAs बनाने की रूपरेखा प्रदान करता है।

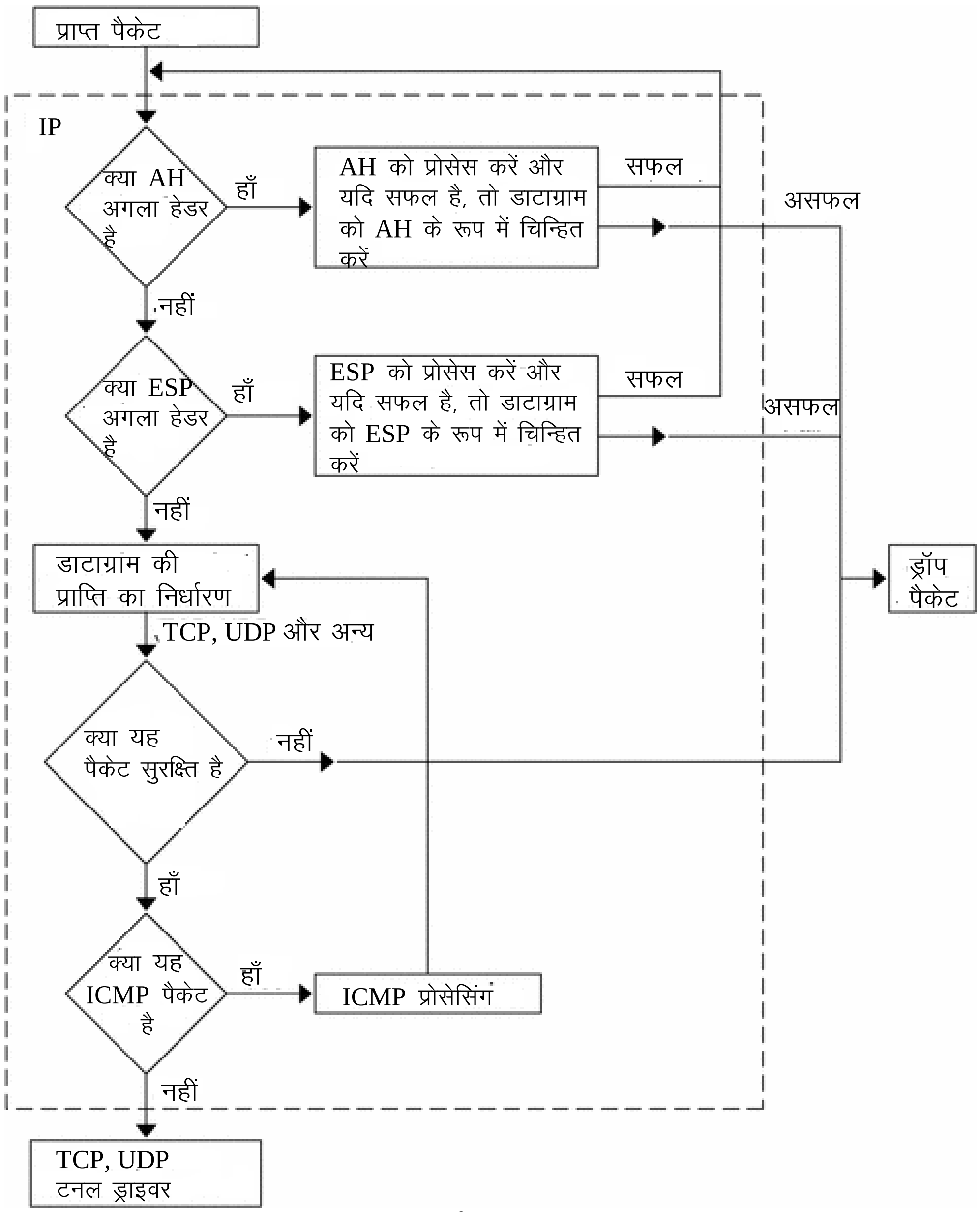
IPsec सुरक्षा तंत्र प्रदान करता है जिसमें IP के अंदर सुरक्षित डेटाग्राम प्रमाणीकरण और एन्क्रिप्शन तंत्र सम्मिलित हैं। जब हम IPsec का आह्वान करते हैं, तो IPsec IP डाटाग्राम पर सुरक्षा तंत्र को लागू करता है जिसे हमने IPsec वैश्विक नीति फाइल में सक्षम किया है। अनुप्रयोग प्रति–सॉकेट स्तर पर IP डेटाग्राम के लिए सुरक्षा तंत्र लागू करने के लिए IPsec को आमंत्रित कर सकते हैं।

निम्न चित्र से पता चलता है कि IP डेटाग्राम के एक हिस्से के रूप में एक IP एड्रेस पैकेट कैसे प्राप्त होता है, जब IPsec को आउटबाउंड पैकेट पर लाया जाता है। जैसा कि हम प्रवाह आरेख से देख सकते हैं, प्रमाणीकरण हेडर (AH) और एन्कैप्सुलेटिंग सिक्योरिटी पेलोड (ESP) इकाइयां पैकेट पर लागू की जा सकती हैं। बाद के अनुभागों का वर्णन है कि हम इन संस्थाओं को कैसे लागू करते हैं, साथ ही प्रमाणीकरण और एन्क्रिप्शन एल्गोरिथ्म।



(चित्र क्र0 11.2)

IPsec इनबाउंड पैकेट प्रक्रियाः



(चित्र क्र0 11.3)

संक्रिया मोडः

IPsec प्रोटोकॉल AH और ESP को होस्ट–से–होस्ट ट्रांसपोर्ट मोड में और साथ ही एक नेटवर्क टनलिंग मोड में लागू किया जा सकता है।

1. ट्रांसपोर्ट मोडः

ट्रांसपोर्ट मोड में, केवल IP पैकेट का पेलोड आमतौर पर एन्क्रिप्ट या प्रमाणित होता है। रूटिंग यथास्थित है, क्योंकि IP हेडर न तो संशोधित है और न ही एन्क्रिप्टेड है।

हालाँकि, जब प्रमाणीकरण शीर्ष लेख का उपयोग किया जाता है, तो IP पते को नेटवर्क पते अनुवाद द्वारा संशोधित नहीं किया जा सकता है, क्योंकि यह सदैव हैश मान को अमान्य करता है।

ट्रांसपोर्ट और एप्लीकेशन परतों को सदैव हैश द्वारा सुरक्षित किया जाता है, इसलिए उन्हें किसी भी तरह से संशोधित नहीं किया जा सकता है, उदाहरण के लिए पोर्ट नंबर का अनुवाद करके।

NAT ट्रावर्सल के लिए IPsec संदेशों को एनकैप्सुलेट करने का एक साधन NAT-T तंत्र का वर्णन करने वाले RFC दस्तावेजों द्वारा परिभाषित किया गया है।

2. टनल मोडः

टनल मोड में, पूरे IP पैकेट को एन्क्रिप्ट और प्रमाणित किया जाता है। इसके बाद एक नए IP हेडर के साथ एक नए IP पैकेट में एनकैप्सुलेट किया जाता है। नेटवर्क–से–नेटवर्क संचार के लिए वर्चुअल प्राइवेट नेटवर्क बनाने के लिए टनल मोड का उपयोग किया जाता है (उदाहरण के लिए लिंक साइट्स के राउटर के मध्य), होस्ट–से–नेटवर्क संचार (जैसे दूरस्थ उपयोगकर्ता एक्सेस) और होस्ट–से–होस्ट संचार (उदाहरण व्यक्तिगत चैट)। टनल मोड NAT ट्रेवर्सल का समर्थन करता है।

जब हम डेटाग्राम की सुरक्षा के लिए IP हेडर के बाद ESP या AH को लागू करते हैं, तो हम ट्रांस्पोर्ट मोड का उपयोग कर रहे हैं। एक उदाहरण इस प्रकार है। एक पैकेट निम्नलिखित हेडर के साथ आरंभ होता हैः

IP Hdr	TCP Hdr	

ESP, ट्रांस्पोर्ट मोड में, निम्नानुसार डेटा की सुरक्षा करता हैः

IP Hdr	ESP	TCP Hdr	

AH, ट्रांस्पोर्ट मोड में, निम्नानुसार डेटा की सुरक्षा करता हैः

IP Hdr	AH	TCP Hdr	

डाटाग्राम में डेटा दिखाई देने से पूर्व AH वास्तव में डेटा को कवर करता है। परिणामतः, AH द्वारा प्रदान की जाने वाली सुरक्षा, यहाँ तक कि परिवहन मोड में, IP हेडर में से कुछ को कवर करती है।

जब एक संपूर्ण डेटाग्राम एक IPsec हेडर के संरक्षण के अंदर होता है, तो IPsec टनल मोड में डेटाग्राम की रक्षा कर रहा है। क्योंकि AH अपने पूर्ववर्ती IP शीर्षकों में से अधिकांश को कवर करता है, टनल मोड आमतौर पर केवल ESP पर किया जाता है। पिछला उदाहरण डेटाग्राम को टनल मोड में संरक्षित करता हैः

IP Hdr	ESP	IP Hdr	TCP Hdr

टनल मोड में, आंतरिक हेडर सुरक्षित है, जबकि वाह्य IP हेडर असुरक्षित है। अक्सर, वाह्य IP हेडर में आंतरिक IP हेडर से अलग स्रोत और विभिन्न गंतव्य पते होते हैं। उदाहरण के लिए, आंतरिक और वाह्य IP हेडर सुमेल कर सकते हैं, उदाहरण के लिए, एक IPsec जागरूक नेटवर्क प्रोग्राम ESP के साथ स्व–एनकैप्सुलेशन का उपयोग करता है। ESP के साथ स्व–एनकैप्सुलेशन एक IP हेडर विकल्प की सुरक्षा करता है।

IPsec का सोलारिस कार्यान्वयन मुख्य रूप से ट्रांस्पोर्ट मोड में IPsec का कार्यान्वयन है। टनल मोड को ट्रांस्पोर्ट मोड के एक विशेष उदाहरण के रूप में लागू किया जाता है। कार्यान्वयन आईपी–इन–आईपी टनल को एक विशेष ट्रांस्पोर्ट प्रदाता के रूप में मानता है। टनल को व्यवस्थित करने के लिए ifconfig(1M) कॉन्फिगरेशन विकल्प लगभग उन विकल्पों के समान है जो सॉकेट प्रोग्रामर के लिए उपलब्ध होते हैं जब प्रति सॉकेट IPsec सक्षम करते हैं। इसके अतिरिक्त, टनल मोड प्रति सॉकेट IPsec में सक्षम किया जा सकता है। प्रति सॉकेट टनल मोड में, आंतरिक पैकेट IP हेडर में वाह्य IP हेडर के समान पते होते हैं।

विश्वसनीय टनलः

एक कॉन्फिगर टनल एक बिंदु–से–बिंदु इंटरफेस है। टनल एक IP पैकेट को IP पैकेट के अंदर एनकैप्सुलेट करने में सक्षम बनाता है। सही ढंग से कॉन्फिगर की गई टनल के लिए टनल स्रोत और टनल गंतव्य दोनों की आवश्यकता होती है।

एक टनल IP के लिए एक स्पष्ट भौतिक इंटरफेस बनाता है। भौतिक लिंक की अखंडता अंतर्निहित सुरक्षा प्रोटोकॉल पर निर्भर करती है। यदि हम सुरक्षा संघों को सुरक्षित रूप से स्थापित करते हैं, तो हम टनल पर भरोसा कर सकते हैं। टनल से बाहर निकलने वाले पैकेट्स की उत्पत्ति टनल गंतव्य में निर्दिष्ट सहकर्मी से हुई होगी। यदि यह विश्वास उपलब्ध है, तो हम वर्चुअल प्राइवेट नेटवर्क बनाने के लिए प्रति–इंटरफेस IP का उपयोग कर सकते हैं।

11.3 IPsec कम्यूनिकेशन (संचार) मोडः

IPsec संचार के कार्य करने की दो विधियाँ हैंः ट्रांस्पोर्ट और टनल मोड। ये मोड संयोजन में उपयोग किए जा सकते हैं या व्यक्तिगत रूप से वांछित संचार के प्रकार के आधार पर उपयोग किए जा सकते हैं।

ट्रांसपोर्ट मोडः

- IPsec ऊपरी परत से प्राप्त पैकेट को एनकैप्सुलेट नहीं करता है।
- मूल IP हेडर बनाए रखा जाता है और ऊपरी परत प्रोटोकॉल द्वारा निर्धारित मूल विशेषताओं के आधार पर डेटा अग्रेषित किया जाता है।
- निम्नलिखित आरेख प्रोटोकॉल स्टैक में डेटा प्रवाह को दर्शाता है।

नेटवर्क	IP हेडर	TCP हेडर	डाटा		
	IP हेडर	←	TCP हेडर	डाटा	
	IP हेडर	ESP/AH	TCP हेडर	डाटा	ESP TRL
	IP हेडर	ESP/AH	TCP हेडर	डाटा	ESP TRL

(चित्र क्र0 11.4)

- ट्रांस्पोर्ट मोड की सीमा यह है कि कोई प्रवेश द्वार सेवाएं प्रदान नहीं की जा सकती हैं। यह बिंदु से बिंदु संचार के लिए आरक्षित है।

टनल मोडः

नेटवर्क	IP हेडर	TCP हेडर	डाटा			
	ESP/AH	IP हेडर	TCP हेडर	डाटा	ESP TRL	
	IP हेडर	ESP/AH	IP हेडर	TCP हेडर	डाटा	ESP TRL
	IP हेडर	ESP/AH	IP हेडर	TCP हेडर	डाटा	ESP TRL

(चित्र क्र0 11.5)

- IPsec का यह मोड अन्य सुरक्षा सेवाओं के साथ एनकैप्सुलेशन सेवाएं प्रदान करता है।
- टनल मोड संचालन में, सुरक्षा प्रोटोकॉल लागू करने से पहले ऊपरी परत से पूरे पैकेट को समझाया जाता है। नया IP हेडर जोड़ा गया है।
- उपरोक्त आरेख प्रोटोकॉल स्टैक में डेटा प्रवाह को दर्शाता है।
- टनल मोड आमतौर पर गेटवे गतिविधियों से जुड़ा होता है। इनकैप्सुलेशन एक गेटवे के माध्यम से कई सत्र भेजने की क्षमता प्रदान करता है।
- जहाँ तक अंत बिन्दु का प्रश्न है, उनका सीधा ट्रांसपोर्ट लेयर कनेक्शन है। गेटवे को अग्रेषित की गई एक प्रणाली के डेटाग्राम को एनकैप्सुलेट किया जाता है और फिर रिमोट गेटवे को अग्रेषित किया जाता है। रिमोट से जुड़े गेटवे डेटा को डि–एनकैप्सुलेट करता है और आंतरिक नेटवर्क पर गंतव्य समापन बिंदु तक आगे बढ़ाता है।
- IPsec का उपयोग करते हुए, टनल मोड को गेटवे और व्यक्तिगत अंत प्रणाली के मध्य भी स्थापित किया जा सकता है।

11.4 IPsec प्रोटोकॉल (संदेशाचार):

IPsec वांछित सुरक्षा सेवाएँ प्रदान करने के लिए सुरक्षा प्रोटोकॉल का उपयोग करता है। ये प्रोटोकॉल IPsec संचालन के दिल हैं और बाकी सब कुछ IPsec में इन प्रोटोकॉल का समर्थन करने के लिए डिजाइन किया गया है।

संचार संस्थाओं के मध्य सुरक्षा संघों का उपयोग सुरक्षा प्रोटोकॉल द्वारा स्थापित और बनाए रखा जाता है। IPsec द्वारा परिभाषित दो सुरक्षा प्रोटोकॉल हैं – प्रमाणीकरण हेडर (AH) और इनकैप्सुलेटिंग सिक्योरिटी पेलोड (ESP)।

प्रमाणीकरण हैडरः

AH प्रोटोकॉल डेटा अखंडता और मूल प्रमाणीकरण की सेवा प्रदान करता है। यह वैकल्पिक रूप से संदेश रिप्ले प्रतिरोध के लिए पूरा करता है। हालांकि, यह गोपनीयता का कोई भी रूप प्रदान नहीं करता है।

AH एक ऐसा प्रोटोकॉल है जो हेडर के अतिरिक्त किसी भी डाटाग्राम की सामग्री के सभी या कुछ भाग का प्रमाणीकरण प्रदान करता है। शीर्ष लेख की गणना डेटाग्राम में मानों के आधार पर की जाती है। डेटाग्राम के किन हिस्सों का उपयोग गणना के लिए किया जाता है, और हेडर को कहाँ रखा जाता है, यह मोड सहयोग (टनल या ट्रांस्पोर्ट) पर निर्भर करता है।

AH प्रोटोकॉल का संचालन आश्चर्यजनक रूप से सरल है। इसे चेकसम की गणना करने या त्रुटि का पता लगाने के लिए CRC का परीक्षण करने हेतु उपयोग किए जाने वाले एल्गोरिथ्म के समान माना जा सकता है।

AH के पीछे की अवधारणा समान है, सिवाय इसके कि एक साधारण एल्गोरिथ्म का उपयोग करने के बजाय, AH विशेष हैशिंग एल्गोरिथ्म का उपयोग करता है और एक गुप्त कुंजी जो केवल संचार दलों के लिए जाना जाता है। दो उपकरणों के मध्य एक सुरक्षा संघ स्थापित किया गया है जो इन विवरणों को निर्दिष्ट करता है।

AH क्यों?

कई दशाओं में, हमारे डेटा को केवल प्रमाणीकरण की आवश्यकता होती है। जबकि एन्कैप्सुलेटिंग सिक्योरिटी पेलोड (ESP) प्रोटोकॉल प्रमाणीकरण कर सकता है, AH हमारे सिस्टम के प्रदर्शन को प्रभावित नहीं करता है जैसा कि ESP करता है। AH का उपयोग करने का एक और लाभ यह है कि AH पूरे डेटाग्राम को प्रमाणित करता है। ESP, हालांकि, प्रमुख IP हेडर या ESP हेडर से पहले आने वाली किसी भी अन्य जानकारी को प्रमाणित नहीं करता है।

इसके अतिरिक्त, ESP को प्रभावी क्रिप्टोग्राफिक एल्गोरिथ्म की आवश्यकता होती है ताकि इसे लागू किया जा सके। कुछ क्षेत्रों में मजबूत क्रिप्टोग्राफी प्रतिबंधित है, जबकि AH विनियमित नहीं है और दुनिया भर में स्वतंत्र रूप से इस्तेमाल किया जा सकता है।

AH की प्रक्रिया निम्नलिखित चरणों से गुजरती हैः

- जब ऊपरी पैकेट स्टैक से IP पैकेट प्राप्त होता है, तो पैकेट में उपलब्ध जानकारी से IPsec संबंधित सुरक्षा एसोसिएशन (SA) निर्धारित करता है। उदाहरण के लिए, IP पता (स्रोत और गंतव्य)।
- SA से, एक बार यह पहचानने के बाद कि सुरक्षा प्रोटोकॉल AH है, AH हेडर के मापदंडों की गणना की जाती है। AH हेडर में निम्नलिखित पैरामीटर होते हैंः

अगला हेडर	पेलोड लंबाई	आरक्षित
सुरक्षा पैरामीटर सूचकांक (SPI)		
अनुक्रम संख्या क्षेत्र		
प्रमाणीकरण डेटा		

- हेडर क्षेत्र AH हेडर के बाद पैकेट के प्रोटोकॉल को निर्दिष्ट करता है। संवाद पक्षों के मध्य उपलब्ध SA से सुरक्षा पैरामीटर सूचकांक (SPI) प्राप्त किया जाता है। अनुक्रम संख्या की गणना की जाती है और प्रविष्ट किया जाता है। ये संख्या रिप्ले हमले का विरोध करने के लिए AH को वैकल्पिक क्षमता प्रदान करते हैं।
- प्रमाणीकरण मोड के आधार पर प्रमाणीकरण डेटा की गणना पृथक–पृथक की जाती है।
- ट्रांस्पोर्ट मोड में, प्रमाणीकरण डेटा की गणना और ट्रांसमिशन के लिए अंतिम IP पैकेट का संयोजन किया जाता है। मूल IP हेडर में, AH के संकेतित एप्लिकेशन के लिए केवल प्रोटोकॉल संख्या 51 में परिवर्तन किया जाता है।

यहाँ पर उपरोक्त का विवरण निम्नानुसार हैः

अगला हेडर: अगला हेडर फील्ड अगले प्रोटोकॉल हेडर की ओर इंगित करता है जो AH हेडर का अनुसरण करता है। यह एक एनकैप्सुलेटिंग सिक्योरिटी पेलोड (ESP) हेडर, एक TCP हेडर या एक UDP हेडर (नेटवर्क एप्लिकेशन के आधार पर) हो सकता है।

पेलोड की लंबाईः 32–बिट शब्दों (4–बाइट इकाइयों) में AH की लंबाई, – 2 निर्दिष्ट करता है।

आरक्षितः यह क्षेत्र वर्तमान में 0 पर सेट है, भविष्य के उपयोग के लिए आरक्षित है।

सुरक्षा पैरामीटर सूचकांक (SPI): सुरक्षा पैरामीटर सूचकांक फील्ड में सुरक्षा पैरामीटर सूचकांक सम्मिलित होता है, इस पैकेट को प्रमाणित करने के लिए उपयोग किए जाने वाले सुरक्षा संघ की पहचान करने के लिए इसका उपयोग किया जाता है।

अनुक्रम संख्याः अनुक्रम संख्या क्षेत्र वर्तमान SA का उपयोग करके प्रेषक से प्राप्तकर्त्ता को भेजे गए संदेशों की संख्या है। काउंटर का प्रारंभिक मान 1 है। इस क्षेत्र का कार्य आवश्यकता होने पर पुनः सुरक्षा को सक्षम करना है।

प्रमाणीकरण डेटाः प्रमाणीकरण डेटा क्षेत्र में इंटीग्रिटी चेक मान गणना का परिणाम होता है, जिसका उपयोग प्राप्तकर्त्ता द्वारा पैकेट के प्रमाणीकरण और अखंडता का परीक्षण करने के लिए किया जा सकता है। इस क्षेत्र को AH की कुल लंबाई बनाने के लिए पैडेड किया जाता है जो कि 32–बिट शब्दों की सटीक संख्या है। RFC 2402 के लिए आवश्यक है कि सभी AH कार्यान्वयन कम से कम HMAC-MD5-96 और HMAC-SHA1-96 का समर्थन करें।

प्रमाणीकरण हैडर (AH) प्रणालीः

प्रमाणीकरण हैडर जानकारी को पैकेट में जोड़ा जाता है, जो कि नेटवर्क (लेयर 3) और ट्रांसपोर्ट (लेयर 4) लेयर (नीचे चित्र देखें) के मध्य प्रेषक द्वारा जनित किया जाता है।

प्रमाणीकरण हमारे नेटवर्क की सुरक्षा करता है, और डेटा जो इसे छेड़छाड़ से बचाता है। छेड़छाड़ क्लाइंट और सर्वर के मध्य बैठा हैकर हो सकता है, क्लाइंट और सर्वर के मध्य भेजे गए पैकेट की सामग्री को बदल सकता है, या कोई क्लाइंट या सर्वर को लगाने की कोशिश कर सकता है, इस प्रकार दूसरे पक्ष को मूर्ख बनाकर संवेदनशील डेटा तक पहुँच प्राप्त कर सकता है।

इस समस्या को दूर करने के लिए, IPSec प्रत्येक पैकेट की संपूर्ण सामग्री को डिजिटल रूप से हस्ताक्षर करने के लिए एक प्रमाणीकरण हैडर का उपयोग करता है। यह हस्ताक्षर 3 लाभ प्रदान करता हैः
1. रिप्ले हमलों के विरूद्व सुरक्षा करता है। यदि कोई हमलावर पैकेट पर कब्जा कर सकता है, उन्हें बचा सकता है और उन्हें संशोधित कर सकता है, और फिर उन्हें गंतव्य पर भेज सकता है, तो वे एक मशीन को तब स्थापित कर सकते हैं जब वह मशीन नेटवर्क पर न हो। इसे ही हम रिप्ले हमला कहते हैं। IPSec इसे सभी पैकेट्स पर प्रेषक के हस्ताक्षर को सम्मिलित करने से रोकेगा।
2. छेड़छाड़ के विरूद्व संरक्षण। IPSec द्वारा प्रत्येक पैकेट में जोड़े गए हस्ताक्षरों का अर्थ है कि हम पैकेट के किसी भी भाग को अनपेक्षित रूप से नहीं बदल सकते हैं।
3. स्पूफिंग के विरूद्व सुरक्षा। एक कनेक्शन का प्रत्येक छोर (जैसे क्लाइंट–सर्वर) IPSec द्वारा उपयोग किए जाने वाले प्रमाणीकरण हेडर के साथ दूसरे की पहचान की पुष्टि करता है।

AH की गणना पूरे पैकेट पर की जाती है, जिसमें पॉलीलोड (ऊपरी परत – 4, 5, 6, 7) और प्रत्येक परत के हेडर सम्मिलित हैं। निम्न चित्र हमें AH का उपयोग करते हुए एक पैकेट दिखाता है।

AH एल्गोरिथ्मः

AH उस एल्गोरिथ्म का उपयोग करता है जिसे हैशेड संदेश प्रमाणीकरण कोड (HMAC) के रूप में जाना जाता है। विशेष रूप से, VPN, HMAC-MD5, HMAC-SHA, HMAC-SHA-256 या AES-XCBC-MAC का उपयोग करता है। एल्गोरिथ्म में से प्रत्येक चर–लंबाई इनपुट डेटा और एक गुप्त कुंजी को निश्चित–लंबाई आउटपुट डेटा (एक हैश या MAC मान कहा जाता है) का जनन करने के लिए लेते हैं। यदि दो संदेशों का हैश मेल करता है, तो यह संभावना है कि संदेश समान हैं।

पॉइंट–से–पॉइंट कम्युनिकेशन (उदाहरण के लिए सर्वर), उपयुक्त प्रमाणीकरण एल्गोरिथ्म में सममित एन्क्रिप्शन एल्गोरिथ्म (उदाहरण के लिए DES) या वन–वे हैश फंक्शंस (जैसे MD5 या SHA–1) पर आधारित कुंजी संदेश प्रमाणीकरण कोड (MAC) सम्मिलित हैं। मल्टीकास्ट संचार के लिए (जैसे राउटर के एक समूह के मध्य), असममित हस्ताक्षर एल्गोरिथ्म के साथ संयुक्त एक तरफा हैश एल्गोरिथ्म आमतौर पर उपयोग किया जाता है, लेकिन वे भी अधिक CPU गहन हैं।

AH, RFC 2402 में परिभाषित, AH, IPv4 और IPv6 पैकेट के लिए कनेक्शन रहित अखंडता और डेटा मूल प्रमाणीकरण प्रदान करता है। यह रिप्ले के विरूद्व सुरक्षा भी प्रदान करता है। AH संभव के रूप में IP हेडर के साथ–साथ ऊपरी–स्तरीय प्रोटोकॉल डेटा को प्रमाणित करता है। हालाँकि, कुछ IP हेडर क्षेत्र परिवर्तन में बदल सकते हैं। चूँकि प्रेषक द्वारा इन क्षेत्रों के मान का अनुमान नहीं लगाया जा सकता है, अतः उन्हें AH द्वारा संरक्षित नहीं किया जा सकता है। IP हेडर में, AH को IPv4 पैकेट के प्रोटोकॉल क्षेत्र में 51 के मान और IPv6 पैकेट के अगले हेडर क्षेत्र के साथ पहचाना जा सकता है। AH द्वारा की पेशकश IPsec सुरक्षा का एक उदाहरण निम्न प्रकार दिखाया गया है।

हेडर फॉर्मेटः

<table>
<tr><td>बाइट 0</td><td colspan="2">बाइट 1</td><td>बाइट 2</td><td colspan="2">बाइट 3</td></tr>
<tr><td colspan="2">अगला हेडर</td><td colspan="2">पेलोड लंबाई</td><td colspan="2">आरक्षित</td></tr>
<tr><td colspan="6">सुरक्षा पैरामीटर सूचकांक (SPI)</td></tr>
<tr><td colspan="6">अनुक्रम संख्या क्षेत्र</td></tr>
<tr><td colspan="6">प्रमाणीकरण डेटा</td></tr>
</table>

AH के लागू होने के पूर्व मूल IPv4 पैकेटः

मूल IP हेडर	TCP हेडर	डाटा

AH ट्रांस्पोर्ट मोड लागू होने के उपरान्त IPv4 पैकेटः

मूल IP हेडर	AH हेडर	TCP हेडर	डाटा

|◄——— प्रमाणीकरण ———►|

AH टनल मोड लागू होने के उपरान्त IPv4 पैकेटः

नया IP हेडर	AH हेडर	मूल IP हेडर	TCP हेडर	डाटा

|◄——— प्रमाणीकरण ———►|

सीमाएंः

प्रमाणीकरण हेडर पूरे डेटा पैकेट के लिए प्रमाणीकरण, अखंडता, और (जब निर्दिष्ट) एंटी–रीप्ले सुरक्षा प्रदान करते हैं। हालांकि, वे गोपनीयता सुनिश्चित नहीं करते हैं, क्योंकि AH प्रोटोकॉल में डेटा प्रसारण को एन्क्रिप्ट करने के लिए कोई मूल प्रावधान नहीं है। एक प्रमाणीकरण हैडर द्वारा संरक्षित पैकेट संशोधित होने से सुरक्षित हैं, लेकिन वे अभी भी किसी के लिए भी पठनीय हैं जो उन तक पहुँच प्राप्त करने के लिए हो सकता है।

इसलिए ऐसी स्थितियों के लिए जहाँ गोपनीयता की आवश्यकता नहीं है या जहाँ एन्क्रिप्शन पर कानूनी प्रतिबंध लगाया जा सकता है, प्रमाणीकरण हेडर्स एक उपयुक्त समाधान हैं। यदि फिर भी एन्क्रिप्शन की आवश्यकता होती है, तो एक सहायक प्रोटोकॉल जैसे ESP (जो एन्क्रिप्शन सेवा प्रदान करता है) पर विचार किया जाना चाहिए।

ऑथेंटिकेशन हेडर का उपयोग निम्नलिखित करने के लिए किया जा सकता हैः

- IP डेटाग्राम के लिए मजबूत अखंडता सेवाएं प्रदान करना, जिसका अर्थ है कि IP डेटाग्राम के लिए सामग्री सत्यापन डेटा ले जाने के लिए AH का उपयोग किया जा सकता है।
- IP डेटाग्राम के लिए मजबूत प्रमाणीकरण प्रदान करना, जिसका अर्थ है कि AH को डेटाग्राम की सामग्री के साथ एक इकाई को जोड़ने के लिए उपयोग किया जा सकता है।
- IP डेटाग्राम के लिए अप्रतिदेय प्रदान करना, यह मानते हुए कि एक सार्वजनिक कुंजी डिजिटल हस्ताक्षर एल्गोरिथ्म का उपयोग अखंडता सेवाओं के लिए किया जाता है।
- अनुक्रम संख्या फील्ड के उपयोग के माध्यम से रिप्ले हमलों से रक्षा करना।

ऑथेंटिकेशन हेडर का उपयोग टनल मोड या ट्रांसपोर्ट मोड में किया जा सकता है, जिसका अर्थ है कि इसका उपयोग दो नोड्स के मध्य सरल, प्रत्यक्ष डेटाग्राम ट्रांसफर को प्रमाणित और संरक्षित करने के लिए किया जा सकता है, या इसका उपयोग डेटाग्राम की एक पूरी स्ट्रीम को एनकोड करने के लिए किया जा सकता है जिसे भेजा जाता है या एक सुरक्षा द्वार से।

ट्रांसपोर्ट मोड में, ऑथेंटिकेशन हैडर मूल IP डेटाग्राम के पेलोड के साथ–साथ IP हैडर के उन भागों की सुरक्षा करता है जो हॉप से हॉप (जैसे, हॉप लिमिट फील्ड या राउटिंग हेडर्स) में नहीं बदलते हैं। नीचे दिया गया चित्र दिखाता है कि ट्रांसपोर्ट मोड IP डेटाग्राम का क्या होता है क्योंकि ऑथेंटिकेशन हैडर की गणना की जाती है और इसे जोड़ा जाता है (डेस्टिनेशन ऑप्शन हेडर ऑथेंटिकेशन हेडर के पूर्व भी प्रकट हो सकता है)। गंतव्य IP पता और विस्तार शीर्ष केवल सुरक्षित हैं क्योंकि वे हॉप से हॉप में नहीं बदलते हैं।

एनकैप्सुलेशन सिक्योरिटी प्रोटोकॉल (ESP):

ESP गोपनीयता, अखंडता, मूल प्रमाणीकरण और वैकल्पिक रिप्ले प्रतिरोध जैसी सुरक्षा सेवाएं प्रदान करता है। प्रदान की गई सेवाओं का समूह सुरक्षा एसोसिएशन (SA) की स्थापना के समय चुने गए विकल्पों पर निर्भर करता है।

ESP में, एन्क्रिप्शन बनाने और प्रमाणिकता जनित करने के लिए उपयोग किए जाने वाले एल्गोरिथ्म SA को बनाने के लिए उपयोग की जाने वाली विशेषताओं से निर्धारित होते हैं। ईएसपी की प्रक्रिया इस प्रकार है। ऊपर बताए अनुसार पहले दो चरण AH की प्रक्रिया के समान हैं।

एक बार जब यह निर्धारित हो जाता है कि ESP सम्मिलित है, तो ESP पैकेट के क्षेत्रों की गणना की जाती है। ESP क्षेत्र व्यवस्था को निम्न चित्र में दर्शाया गया है।

सुरक्षा पैरामीटर सूचकांक (SPI)		
अनुक्रम संख्या क्षेत्र		
एन्क्रिप्टेड पेलोड		
पैडिंग	पैड लंबाई	अगला हेडर
प्रमाणीकरण डेटा		

निम्नलिखित ESP हैडर प्रारूप (आरएफसी 2406 से लिया गया) में अगला हैडर क्षेत्र सम्मिलित है, जो ESP हैडर के अंत के पास दिखाई देता है और किसी भी अन्य हेडर (जैसे AH) की उपस्थिति (और पहचान) को इंगित करता है जो अनुसरण कर सकते हैं। ESP हेडर के अन्य भागों में निम्नलिखित सम्मिलित हैं।

सुरक्षा पैरामीटर इंडेक्स (SPI): यह वही 32–बिट मान है जिसे प्रमाणीकरण हेडर संदर्भित किया गया है। इस मान का उपयोग संचार नोड्स द्वारा एक सुरक्षा संघ को संदर्भित करने के लिए किया जाता है, जिसका उपयोग यह निर्धारित करने के लिए किया जा सकता है कि डेटा को कैसे एन्क्रिप्ट किया जाना चाहिए।

अनुक्रम संख्याः इस 32–बिट मान को आरंभ करने के लिए शून्य पर व्यवस्थित किया गया है और प्रत्येक भेजे गए डेटाग्राम के साथ एक के बाद एक बढ़ा हुआ है। जैसा कि ऑथेंटिकेशन हेडर के लिए वर्णित है, रिप्ले हमलों से बचाने के लिए अनुक्रम संख्या का उपयोग किया जा सकता है, और सभी 32 मानों के माध्यम से इस मूल्य चक्र से पहले एक नया सुरक्षा संघ स्थापित किया जाना चाहिए।

पेलोड डेटाः यह एक वैरिएबल–लेंथ क्षेत्र है और वास्तव में डेटाग्राम के एन्क्रिप्टेड भाग के साथ–साथ एन्क्रिप्शन एल्गोरिथ्म (जैसे, आरंभीकरण डेटा) के लिए आवश्यक किसी भी पूरक डेटा के साथ है। पेलोड एक आरंभीकरण वेक्टर के साथ आरंभ होता है, एक मान जिसे प्लेन–टेक्स्ट में भेजा जाना चाहिए, एन्क्रिप्शन एल्गोरिथ्म को संरक्षित डेटा को डिक्रिप्ट करने के लिए इस मान की आवश्यकता होती है।

पैडिंगः हेडर (पेलोड) के एन्क्रिप्टेड भाग को उचित सीमा पर समाप्त होना चाहिए, इसलिए पैडिंग आवश्यक हो सकती है।

पैडिंग लंबाईः यह फील्ड इंगित करता है कि पेलोड डेटा में कितना पैडिंग जोड़ा गया है।

अगला हैडर: यह फील्ड सामान्य रूप से अन्य IPv6 एक्सटेंशन हेडर के साथ काम करता है। यह सिर्फ हेडर के अंत के पास दिखाई देता है (जहाँ इसे गोपनीयता की सुरक्षा दी जा सकती है) बजाय आरंभ में ताकि अगली लेयर प्रोटोकॉल को किसी भी अनाधिकृत तीसरे पक्ष से छिपाया जा सके।

प्रमाणीकरण डेटाः यह संपूर्ण ESP हैडर (प्रमाणीकरण डेटा को छोड़कर) पर गणना किया गया एक अखंडता परीक्षण मान (ICV) है। यह प्रमाणीकरण गणना वैकल्पिक है। ICV की चर्चा अधिक लंबाई के बाद की जाती है।

हालांकि प्रमाणीकरण और गोपनीयता ESP द्वारा प्रदान की जाने वाली प्राथमिक सेवाएं हैं, दोनों वैकल्पिक हैं। तकनीकी रूप से, हम प्रमाणीकरण के बिना NULL एन्क्रिप्शन का उपयोग कर सकते हैं। हालांकि, व्यवहार में, ESP का प्रभावी ढंग से उपयोग करने के लिए दोनों में से एक को लागू किया जाना चाहिए। मूल अवधारणा ESP का उपयोग करना है जब कोई प्रमाणीकरण और एन्क्रिप्शन चाहता है, और AH का उपयोग करने के लिए जब कोई एन्क्रिप्शन के बिना विस्तारित प्रमाणीकरण चाहता है।

इनकैप्सुलेटिंग सिक्योरिटी पेलोड (ESP):

हमने जिस प्रमाणीकरण हेडर (AH) के बारे में बात की थी, वह हमारे डेटा को छेड़छाड़ से बचाएगा, लेकिन यह लोगों को इसे देखने से नहीं रोकेगा। उसके लिए, IPSec एक एन्क्रिप्शन का उपयोग करता है जो एन्कैप्सुलेटिंग सिक्योरिटी पेलोड (ESP) प्रदान करता है।

ESP का उपयोग IPSec पैकेट के पूरे पेलोड को एन्क्रिप्ट करने के लिए किया जाता है (पेलोड पैकेट का वह भाग होता है जिसमें ऊपरी परत डेटा होता है)।

ESP, AH की तुलना में थोड़ा अधिक जटिल है क्योंकि अकेले ही यह प्रमाणीकरण, रिप्ले–प्रूफिंग और अखंडता जाँच प्रदान कर सकता है। यह 3 अलग–अलग घटकों को जोड़कर इसका संयोजन करता हैः एक ESP हेडर, एक ESP ट्रेलर और एक ESP प्रमाणीकरण ब्लॉक।

इनमें से प्रत्येक घटक में आवश्यक प्रमाणीकरण और अखंडता जाँच प्रदान करने के लिए आवश्यक कुछ डेटा शामिल हैं। छेड़छाड़ को रोकने के लिए, एक ESP क्लाइंट को ESP हेडर, एप्लिकेशन डेटा और ESP ट्रेलर को एक इकाई में हस्ताक्षर करना होता है, निश्चित रूप से ESP का उपयोग गोपनीयता प्रदान करने के लिए एप्लिकेशन डेटा और ESP ट्रेलर को एन्क्रिप्ट करने के लिए किया जाता है। इस अतिव्यापी हस्ताक्षर और एन्क्रिप्शन संक्रिया का संयोजन अच्छी सुरक्षा प्रदान करता है। ESP, RFC 2406 में परिभाषित है, ESP एन्क्रिप्शन और सीमित ट्रैफिक प्रवाह गोपनीयता या कनेक्शन रहित अखंडता, डेटा उत्पत्ति प्रमाणीकरण और एक एंटी–रीप्ले सेवा प्रदान कर सकता है। एक IP हेडर में, ESP को एक IPv4 पैकेट के प्रोटोकॉल क्षेत्र में 50 के मान और एक IPv6 पैकेट के अगले हेडर फील्ड के रूप में पहचाना जा सकता है। ESP द्वारा की गई पेशकश IPsec संरक्षण का एक उदाहरण निम्न चित्र में दिखाया गया है।

हेडर फॉर्मेटः

बाइट 0	बाइट 1	बाइट 2	बाइट 3
सुरक्षा पैरामीटर सूचकांक (SPI)			
अनुक्रम संख्या			
पेलोड डाटा			
पैडिंग (0-255)	पैड लंबाई	अगला हेडर	
प्रमाणीकरण डेटा			

ESP के लागू होने के पूर्व मूल IPv4 पैकेटः

मूल IP हेडर	TCP हेडर	डाटा

ESP ट्रांस्पोर्ट मोड लागू होने के उपरान्त IPv4 पैकेटः

मूल IP हेडर	ESP हेडर	TCP हेडर	डाटा	ESP हेडर	ESP प्राधिकरण

|← एनक्रिप्टेड →|

|← प्रमाणीकरण →|

ESP टनल मोड लागू होने के उपरान्त IPv4 पैकेटः

नया IP हेडर	ESP हेडर	मूल IP हेडर	TCP हेडर	डाटा	ESP ट्रालर	ESP प्रमाणीकरण

|← एनक्रिप्टेड →|

|← प्रमाणीकरण →|

सूचना की सुरक्षा के लिए ESP किस एल्गोरिथ्म का उपयोग करता है?

ESP एक सममित कुंजी का उपयोग करता है जो दोनों संचार पक्षों का उपयोग उनके द्वारा विनिमय किए गए डेटा को एन्क्रिप्ट और डिक्रिप्ट करने के लिए करते हैं। प्रेषक और प्राप्तकर्त्ता को उनके मध्य सुरक्षित संचार होने से पहले कुंजी पर सहमत होना चाहिए।

VPN एन्क्रिप्शन के लिए डेटा एन्क्रिप्शन स्टैंडर्ड (DES), ट्रिपल–DES (3DES), एडवांस्ड एन्क्रिप्शन स्टैंडर्ड (AES), या AES-CBC और AES-CTR का उपयोग करता है।

यदि हम एन्क्रिप्शन के लिए AES एल्गोरिथ्म चुनते हैं तो हम विस्तारित अनुक्रम संख्या (ESN) को सक्षम करना चाह सकते हैं। ESN हमें उच्च गति पर डेटा के बड़े संस्करणों को प्रसारित करने की अनुमति देता है। VPN कनेक्शन IPSec पर 32–बिट संख्याओं के स्थान पर 64–बिट अनुक्रम संख्या का उपयोग करता है। 64–बिट अनुक्रम संख्याओं का उपयोग करने से पुनः कुंजीकरण से पहले अधिक समय की अनुमति मिलती है, जो अनुक्रम संख्या की थकावट को रोकता है और सिस्टम संसाधनों के उपयोग को कम करता है।

बंडलः

जब हम AH की तुलना ESP से करते हैं, तो दोनों प्रोटोकॉल में कुछ लाभ और कमियां होती हैं। ESP प्रमाणीकरण और एन्क्रिप्शन का एक सभ्य स्तर प्रदान करता है, लेकिन ऐसा केवल IP पैकेट के भाग के लिए होता है। इसके विपरीत, हालांकि AH एन्क्रिप्शन प्रदान नहीं करता है, यह पूरे IP पैकेट के लिए प्रमाणीकरण प्रदान करता है। इसके कारण, Junos OS IPsec प्रोटोकॉल का तीसरा रूप प्रदान करता है जिसे प्रोटोकॉल बंडल कहा जाता है। बंडल विकल्प ESP एन्क्रिप्शन के साथ AH प्रमाणीकरण का एक संकर संयोजन प्रदान करता है।

11.5 IPsec में सुरक्षा संघः

सुरक्षा संघ (SA) एक IPsec संचार की नींव है। SA की विशेषताएं निम्न हैंः

- डेटा भेजने से पहले, भेजने वाली इकाई और प्राप्त करने वाली इकाई के मध्य एक वर्चुअल कनेक्शन स्थापित किया जाता है, जिसे सुरक्षा संघ कहा जाता है।
- IPsec नेटवर्क एन्क्रिप्शन और प्रमाणीकरण करने के लिए कई विकल्प प्रदान करता है। प्रत्येक IPsec कनेक्शन एन्क्रिप्शन, अखंडता, प्रामाणिकता या तीनों सेवाएं प्रदान कर सकता है। जब सुरक्षा सेवा निर्धारित की जाती है, तो दो IPsec सहकर्मी संस्थाओं को निश्चित रूप से यह निर्धारित करना चाहिए कि कौन से एल्गोरिथ्म का उपयोग करना है (उदाहरण के लिए, एन्क्रिप्शन के लिए DES या 3DES, अखंडता के लिए MD5 या SHA–1)। एल्गोरिथ्म पर निर्णय लेने के उपरान्त, दोनों उपकरणों को सत्र कुंजियों को साझा करना होगा।
- SA, उपरोक्त संचार मापदंडों का एक समूह है जो IPsec सत्र बनाने के लिए दो या अधिक प्रणालियों के मध्य संबंध प्रदान करता है।
- SA प्रकृति में सरल है और इसलिए द्वि–दिशात्मक संचार के लिए दो SA की आवश्यकता होती है।
- SA की पहचान एक सुरक्षा पैरामीटर इंडेक्स (SPI) संख्या से होती है जो सुरक्षा प्रोटोकॉल हेडर में उपलब्ध होता है।
- दोनों भेजने और प्राप्त करने वाली संस्थाएं SA के बारे में अवस्था की जानकारी बनाए रखती हैं। यह TCP अंत बिन्दु के समान है जो अवस्था की जानकारी भी बनाए रखता है। IPsec, TCP के समान कनेक्शन–उन्मुख है।

SA के पैरामीटरः

किसी भी एसए को अद्वतीय रूप से निम्नलिखित तीन मापदंडों द्वारा पहचाना जाता हैः

1. सिक्योरिटी पैरामीटर्स इंडेक्स (SPI):

- यह SA को दिया गया 32–बिट मान है। यह एक ही गंतव्य पर समाप्त करने और एक ही IPsec प्रोटोकॉल का उपयोग करने वाले विभिन्न SA के मध्य अंतर करने के लिए उपयोग किया जाता है।
- IPsec के प्रत्येक पैकेट में SPI फील्ड वाला हेडर होता है। SPI को आने वाले पैकेट को SA में मैप करने के लिए प्रदान किया जाता है।
- SPI प्राप्तकर्ता को SA की पहचान करने के लिए प्रेषक द्वारा उत्पन्न एक यादृच्छिक संख्या है।

2. डेस्टिनेशन IP एड्रेसः यह अंतिम राउटर का IP एड्रेस हो सकता है।
3. सुरक्षा प्रोटोकॉल पहचानकर्ताः यह इंगित करता है कि क्या एसोसिएशन AH या ESP SA है।

सुरक्षा प्रशासनिक डेटाबेसः

IPsec में, दो डेटाबेस हैं जो IPsec डेटाग्राम के प्रसंस्करण को नियंत्रित करते हैं। एक सुरक्षा संघ डेटाबेस (SAD) है और दूसरा सुरक्षा नीति डेटाबेस (SPD) है। IPsec का उपयोग करने वाले प्रत्येक संचार बिंदु के पास तार्किक रूप से पृथक SAD और SPD होना चाहिए।

सुरक्षा एसोसिएशन डेटाबेसः

IPsec संचार में, अंत बिन्दु SA अवस्था को सुरक्षा संघ डेटाबेस में रखता है। SAD डेटाबेस में प्रत्येक SA प्रविष्टि में नौ पैरामीटर हैं जैसा कि निम्नलिखित तालिका में दिखाया गया हैः

स. क्र.	पैरामीटर और उनका विवरण
1	**अनुक्रम संख्या काउंटर** आउटबाउंड संचार के लिए। यह AH या ESP हेडर में प्रदान किया गया 32–बिट अनुक्रम संख्या है।
2	**अनुक्रम संख्या अतिप्रवाह काउंटर** विशिष्ट SA का उपयोग करते हुए आगे संचार को रोकने के लिए एक विकल्प ध्वज सेट करता है।
3	**32–बिट एंटी–रिप्ले विंडो** यह निर्धारित करने के लिए उपयोग किया जाता है कि एक इनबाउंड AH या ESP पैकेट एक रिप्ले है।
4	**SA का जीवनकाल** SA सक्रिय रहने तक का समय।
5	**एल्गोरिथ्म – AH** AH और संबद्ध कुंजी में उपयोग किया जाता है
6	**एल्गोरिथ्म – ESP प्रामाणीकरण** ESP हेडर के प्रमाणीकरण वाले हिस्से में उपयोग किया जाता है
7	**एल्गोरिथ्म – ESP एन्क्रिप्शन** ESP के एन्क्रिप्शन और उससे जुड़ी प्रमुख जानकारियों में प्रयुक्त
8	**संक्रिया का IPsec मोड** ट्रांस्पोर्ट या टनल मोड
9	**पथ MTU(PMTU)** कोई भी प्रेक्षित किया गया पथ अधिकतम संचरण इकाई (विखंडन से बचने के लिए)

SAD में सभी SA प्रविष्टियों को तीन SA मापदंडों द्वारा अनुक्रमित किया जाता हैः गंतव्य IP पता, सुरक्षा प्रोटोकॉल पहचानकर्ता और SPI।

सुरक्षा नीति डेटाबेस (SPD):

SPD का उपयोग आउटगोइंग पैकेट के प्रसंस्करण के लिए किया जाता है। यह निर्णय लेने में मदद करता है कि SAD प्रविष्टियों का क्या उपयोग किया जाना चाहिए। यदि कोई SAD प्रविष्टि उपलब्ध नहीं है, तो SPD का उपयोग नए बनाने के लिए किया जाता है।

किसी भी SPD प्रविष्टि में शामिल होंगे –

- सक्रिय SA (जो SAD में है) की ओर इंगित करता है।

- **चयनकर्ता फील्डः** ऊपरी परत से आने वाले पैकेट में फील्ड IPsec के एप्लीकेशन को तय करने के लिए उपयोग किया जाता है। चयनकर्ताओं में स्रोत और गंतव्य का पता, पोर्ट नंबर यदि प्रासंगिक हो, एप्लिकेशन ID, प्रोटोकॉल आदि शामिल हो सकते हैं।

आउटगोइंग IP डेटाग्राम एन्कोडिंग मापदंडों को प्राप्त करने के लिए SPD प्रविष्टि से विशिष्ट SA में जाते हैं। आने वाली IPsec डेटाग्राम सही SA को सीधे SPI/DEST IP/प्रोटोकॉल ट्रिपल का उपयोग करते हुए मिलता है, और वहाँ से संबंधित SAD प्रविष्टि को निकालता है।

SPD, IPsec को बायपास करने वाले ट्रैफिक को भी निर्दिष्ट कर सकता है। SPD को एक पैकेट फिल्टर के रूप में माना जा सकता है, जहाँ कार्रवाई का निर्णय SA प्रक्रियाओं की सक्रियता है।

नेटवर्क परत का सार संक्षेपः

IPsec नेटवर्क कनेक्शन हासिल करने के लिए प्रोटोकॉल का एक सूइट है। यह एक जटिल तंत्र है, क्योंकि एक विशिष्ट एन्क्रिप्शन एल्गोरिथ्म और प्रमाणीकरण फंक्शन की सीधी परिभाषा देने के स्थान पर, यह एक ऐसा ढांचा प्रदान करता है जो किसी भी ऑब्जेक्ट के कार्यान्वयन की अनुमति देता है जो दोनों संप्रेषण समाप्त होने पर सहमत होते हैं।

ऑथेंटिकेशन हैडर (AH) और एनकैप्सुलेटिंग सिक्योरिटी पेलोड (ESP) IPsec के द्वारा उपयोग किए जाने वाले दो मुख्य संचार प्रोटोकॉल हैं। जबकि AH केवल प्रमाणित करता है, ESP कनेक्शन पर प्रेषित डेटा को एन्क्रिप्ट और प्रमाणित कर सकता है।

ट्रांसपोर्ट मोड IP हेडर को बदले बिना दो अंत बिन्दुओं के मध्य एक सुरक्षित कनेक्शन प्रदान करता है। टनल मोड पूरे पेलोड IP पैकेट को एनकैप्सुलेट करता है। यह नया IP हेडर जोड़ता है। बाद में इसका उपयोग पारंपरिक VPN बनाने के लिए किया जाता है, क्योंकि यह एक अविश्वसनीय इंटरनेट पर एक आभासी सुरक्षित टनल प्रदान करता है।

IPsec कनेक्शन व्यवस्थित करने में सभी प्रकार की क्रिप्टो विकल्प सम्मिलित हैं। प्रमाणीकरण आमतौर पर एक क्रिप्टोग्राफिक हैश के शीर्ष पर बनाया जाता है जैसे कि MD5 या SHA-1। एन्क्रिप्शन एल्गोरिदम DES, 3DES, Blowfish और AES आम हैं। अन्य एल्गोरिथ्म भी संभव हैं।

दोनों संचार समापन बिंदुओं को हैशिंग या एन्क्रिप्शन में उपयोग किए गए गुप्त मूल्यों को जानने की आवश्यकता है। हस्त कुंजी को दोनों सिरों पर गुप्त मूल्यों के हस्त प्रविष्टि की आवश्यकता होती है, संभवतः कुछ आउट–ऑफ–बैंड तंत्र द्वारा अवगत कराया जाता है, और इंटरनेट की एक्सचेंज (IKE) यह ऑनलाइन करने के लिए एक परिष्कृत तंत्र है।

अभ्यास

1. नेटवर्क लेयर (जालक्रम परत) में सुरक्षा से क्या समझते हैं?
2. IPsec का आकलन कैसे करते हैं?
3. IPsec कम्यूनिकेशन (संचार) मोड पर संक्षिप्त टिप्पणी लिखिए।
4. IPsec प्रोटोकॉल (संदेशाचार) को समझाइए।
5. IPsec में सुरक्षा संघ की अवधारणा को स्पष्ट कीजिए।

अध्याय – 12

डेटा लिंक लेयर
(आंकड़ा कड़ी परत)

हमने देखा है कि इंटरनेट के तेजी से विकास ने नेटवर्क सुरक्षा के लिए एक बड़ी चिंता उत्पन्न कर दी है। किसी नेटवर्क के एप्लिकेशन, ट्रांसपोर्ट या नेटवर्क लेयर में सुरक्षा प्रदान करने के लिए कई विधियाँ विकसित की गई हैं।

कई संगठन उच्चतर OSI परतों में सुरक्षा उपायों को शामिल करते हैं, एप्लीकेशन परत से लेकर IP परत तक सभी तरह से। हालांकि, आमतौर पर अप्राप्य छोड़े गए एक क्षेत्र डेटा लिंक परत का सख्त होना है। यह नेटवर्क को कई तरह के हमलों के लिए खोल सकता है और समझौता कर सकता है।

इस अध्याय में, हम डेटा लिंक लेयर पर सुरक्षा समस्याओं और उनका मुकाबला करने के तरीकों पर चर्चा करेंगे। हमारी चर्चा ईथरनेट नेटवर्क पर केंद्रित होगी।

डेटा परत, या परत 2, कम्प्यूटर नेटवर्किंग के सात–परत OSI मॉडल की दूसरी परत है। यह परत प्रोटोकॉल परत है जो एक विस्तृत क्षेत्र नेटवर्क (WAN) में या एक ही स्थानीय क्षेत्र नेटवर्क (LAN) खंड पर नोड्स के मध्य आसन्न नेटवर्क नोड्स के मध्य डेटा स्थानांतरित करता है। डेटा लिंक परत नेटवर्क संस्थाओं के मध्य डेटा को स्थानांतरित करने के लिए कार्यात्मक और प्रक्रियात्मक साधन प्रदान करता है और भौतिक परत में होने वाली त्रुटियों का पता लगाने और संभवतः सही करने के लिए साधन प्रदान कर सकता है।

डेटा लिंक परत नेटवर्क के समान स्तर पर नोड्स के मध्य फ्रेम के स्थानीय वितरण से संबंधित है। डेटा–लिंक फ्रेम, जैसा कि इन प्रोटोकॉल डेटा इकाइयों को कहा जाता है, किसी स्थानीय क्षेत्र नेटवर्क की सीमाओं को पार नहीं करते हैं। इंटर–नेटवर्क रूटिंग और ग्लोबल एड्रेसिंग उच्च–परत फंक्शन हैं, जो डेटा–लिंक प्रोटोकॉल को स्थानीय डिलीवरी, एड्रेसिंग और मीडिया आर्बिट्रेशन पर ध्यान केंद्रित करने की अनुमति देता है। इस तरह, डेटा लिंक परत पड़ोस ट्रैफिक पुलिस के अनुरूप है, यह अपने अंतिम गंतव्य के लिए चिंता किए बिना एक माध्यम तक पहुँच के लिए संघर्ष करने वाले पक्षों के मध्य मध्यस्थता करने का प्रयास करता है। जब उपकरण एक साथ माध्यम का उपयोग करने का प्रयास करते हैं, तो फ्रेम टकराव होता है। डेटा–लिंक प्रोटोकॉल निर्दिष्ट करते हैं कि कैसे डिवाइस ऐसे टकरावों से पता लगाते हैं और पुनर्प्राप्त करते हैं, और उन्हें कम करने या रोकने के लिए तंत्र प्रदान कर सकते हैं।

डेटा लिंक प्रोटोकॉल के उदाहरण स्थानीय क्षेत्र नेटवर्क (मल्टी–नोड), पॉइंट–टू–पॉइंट प्रोटोकॉल (PPP), HDLC और ADCCP पॉइंट–टू–पॉइंट (डुअल–नोड) कनेक्शन के लिए ईथरनेट हैं। इंटरनेट प्रोटोकॉल सूट (TCP/IP) में, लिंक परत के अंदर डेटा लिंक परत की कार्यक्षमता निहित है, वर्णनात्मक मॉडल की सबसे निचली परत, जिसमें OSI मॉडल की भौतिक परत में शामिल कार्यक्षमता भी सम्मिलित है।

लॉजिकल लिंक कंट्रोल (LLC) सबलेयरः

ऊपरवाला सबलेयर, LLC, मल्टीप्लेक्स प्रोटोकॉल डेटा लिंक लेयर के शीर्ष पर चल रहा है, और वैकल्पिक रूप से फ्लो कंट्रोल, पावती और त्रुटि सूचना प्रदान करता है। LLC डेटा लिंक का पता और नियंत्रण प्रदान करता है। यह निर्दिष्ट करता है कि ट्रांसमिशन माध्यम पर स्टेशन्स को संबोधित करने और प्रवर्तक और प्राप्तकर्ता मशीन्स के मध्य आदान–प्रदान किए गए डेटा को नियंत्रित करने के लिए किन तंत्रों का उपयोग किया जाना है।

मीडिया एक्सेस कंट्रोल (MAC) सबलेयरः

MAC उस उपपरत को संदर्भित कर सकता है जो यह निर्धारित करता है कि मीडिया को किसी भी समय (जैसे CSMA/CD) को एक्सेस करने की अनुमति कौन देता है। दूसरी बार यह MAC के पते पर आधारित एक फ्रेम संरचना को संदर्भित करता है।

आमतौर पर मीडिया एक्सेस कंट्रोल के दो रूप हैंः वितरित और केंद्रीकृत। इन दोनों की तुलना व्यक्तियों के मध्य होने वाले संचार से की जा सकती है। बोलने वाले व्यक्तियों से बने नेटवर्क में, यानी एक वार्तालाप में, वे प्रत्येक समय का एक यादृच्छिक राशि रोकेंगे और फिर से बोलने का प्रयास करेंगे, प्रभावी रूप से 'नहीं, आप पहले' कहने का एक लंबा और विस्तृत खेल स्थापित करेंगे।

मीडिया एक्सेस कंट्रोल सबलेयर यह भी निर्धारित करता है कि डेटा का एक फ्रेम कहाँ समाप्त होता है और अगला कब आरंभ होता है – फ्रेम सिंक्रोनाइजेशन। फ्रेम सिंक्रोनाइजेशन के चार साधन हैं: समय आधारित, वर्ण गणना, बाइट स्टफिंग और बिट स्टफिंग।

डेटा लिंक लेयर के कार्य:

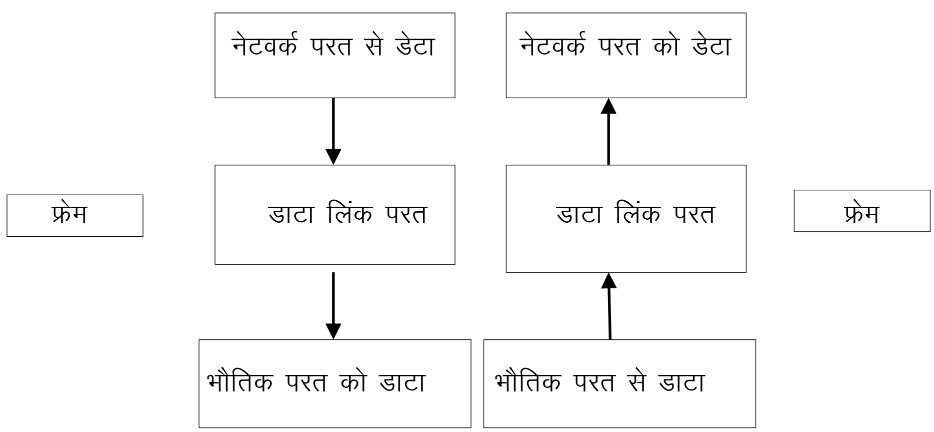
1. फ्रेमिंग: फ्रेम्स नेटवर्क लेयर से प्राप्त बिट्स की स्ट्रीम प्रबंध करने योग्य डेटा यूनिट्स में होते हैं। बिट्स की धारा का यह विभाजन डेटा लिंक लेयर द्वारा किया जाता है।

2. भौतिक पता: डेटा लिंक परत फ्रेम के प्रेषक या प्राप्तकर्त्ता के भौतिक पते को परिभाषित करने के लिए फ्रेम में एक हेडर जोड़ता है, यदि फ्रेम नेटवर्क पर विभिन्न प्रणालियों को वितरित किया जाना हो।

3. फ्लो कंट्रोल: फ्लो कंट्रोल द्वारा एक फास्ट ट्रांसमीटर से बचने के लिए फ्लो कंट्रोल तकनीक, फ्लो कंट्रोल द्वारा अतिरिक्त बिट को बफर करके धीमी रिसीवर को चलाने से बचता है। यह प्राप्तकर्त्ता की तरफ ट्रैफिक जाम को रोकता है।

4. त्रुटि नियंत्रण: फ्रेम के अंत में एक ट्रेलर जोड़कर त्रुटि नियंत्रण हासिल किया जाता है। इस तंत्र का उपयोग करके फ्रेम के दोहराव को भी रोका जाता है। डेटा लिंक परतें फ्रेम के दोहराव को रोकने के लिए तंत्र को जोड़ती हैं।

5. अभिगम नियंत्रण: इस परत के प्रोटोकॉल निर्धारित करते हैं कि किसी भी समय लिंक में से कौन से उपकरण पर नियंत्रण है, जब दो या अधिक उपकरण एक ही लिंक से जुड़े होते हैं।



(चित्र क्र0 12.1)

डेटा लिंक परत के साथ डिजाइन के मुद्दे:

- डेटा लिंक लेयर (और अधिकांश उच्चतर लेयर्स) में जो समस्या उत्पन्न होती है, वह यह है कि डेटा में धीमी रिसीवर को डूबने से फास्ट ट्रांसमीटर कैसे रखा जाए। कुछ ट्रैफिक विनियमन तंत्र को अक्सर ट्रांसमीटर को यह बताने की आवश्यकता होती है कि प्राप्तकर्त्ता के पास कितना बफर स्थान है। अक्सर, प्रवाह विनियमन और त्रुटि से निपटने को एकीकृत किया जाता है।
- प्रसारण नेटवर्क में डेटा लिंक परत में एक अतिरिक्त मुद्दा है, साझा चैनल तक पहुँच को कैसे नियंत्रित किया जाए। डेटा लिंक परत की एक विशेष उप–परत, मीडिया एक्सेस कंट्रोल (MAC) उप–परत, इस समस्या से संबंधित है।

सेवाएं:

डेटा लिंक लेयर द्वारा निम्नलिखित सेवाएं प्रदान की जाती हैं:

फ्रेमिंग और लिंक एक्सेस: डेटा लिंक लेयर प्रोटोकॉल लिंक के प्रसारण से पहले प्रत्येक नेटवर्क फ्रेम को लिंक लेयर फ्रेम के अंदर एन्क्रिप्ट कर देता है। फ्रेम में एक डेटा क्षेत्र होता है जिसमें नेटवर्क लेयर डेटाग्राम और कई डेटा क्षेत्र सम्मिलित होते हैं। यह फ्रेम की संरचना के साथ–साथ एक चैनल एक्सेस प्रोटोकॉल को निर्दिष्ट करता है जिसके द्वारा लिंक पर फ्रेम प्रसारित किया जाना है।

विश्वसनीय वितरणः डेटा लिंक लेयर एक विश्वसनीय वितरण सेवा प्रदान करता है, अर्थात, बिना किसी त्रुटि के नेटवर्क लेयर डेटाग्राम पहुँचाता है। एक विश्वसनीय वितरण सेवा प्रसारण और पावती के साथ पूरी होती है। डेटा लिंक परत मुख्य रूप से लिंक पर विश्वसनीय वितरण सेवा प्रदान करता है क्योंकि उनके पास उच्च त्रुटि दर होती है और उन्हें स्थानीय रूप से ठीक किया जा सकता है, जिस लिंक पर डेटा को पुनः प्राप्त करने के लिए त्रुटि के बजाय कोई त्रुटि उत्पन्न होती है।
प्रवाह नियंत्रणः एक प्राप्त नोड फ्रेम को संसाधित करने की तुलना में तेज दर से प्राप्त कर सकता है। प्रवाह नियंत्रण के बिना, प्राप्तकर्त्ता का बफर अतिप्रवाह कर सकता है, और फ्रेम खो सकता है। इस समस्या को दूर करने के लिए, लिंक के एक ओर भेजने वाले नोड को लिंक के दूसरी ओर भारी होने से रोकने के लिए डेटा लिंक परत प्रवाह नियंत्रण का उपयोग करता है।
त्रुटि का पता लगानाः सिग्नल क्षीणन और शोर द्वारा त्रुटियों को पेश किया जा सकता है। डेटा लिंक लेयर प्रोटोकॉल एक या अधिक त्रुटियों का पता लगाने के लिए एक तंत्र प्रदान करता है। यह फ्रेम में त्रुटि का पता लगाने वाले बिट्स को जोड़कर प्राप्त किया जाता है और फिर नोड प्राप्त करने से त्रुटि का परीक्षण हो सकता है।
त्रुटि सुधारः त्रुटि सुधार त्रुटि का पता लगाने के समान है, सिवाय इसके कि नोड को न केवल त्रुटियों का पता लगाएं, बल्कि यह भी निर्धारित करें कि त्रुटियां फ्रेम में कहाँ हुई हैं।
अर्द्ध–डुप्लेक्स और पूर्ण–डुप्लेक्सः पूर्ण–डुप्लेक्स मोड में, दोनों नोड एक ही समय में डेटा संचारित कर सकते हैं। अर्द्ध–डुप्लेक्स मोड में, केवल एक नोड एक ही समय में डेटा संचारित कर सकता है।

डेटा लिंक लेयर प्रोटोकॉलः

प्रोटोकॉल के दो प्रमुख वर्ग, व्यापक रूप से डेटा लिंक परत द्वारा उपयोग किए जाने वाले बिट–उन्मुख प्रोटोकॉल और कैरेक्टर–उन्मुख प्रोटोकॉल हैं।

1. कैरेक्टर–उन्मुख प्रोटोकॉलः

कैरेक्टर–उन्मुख प्रोटोकॉल जानकारी को संप्रेषित करने के लिए कैरेक्टर्स के पूर्वनिर्धारित सेट का उपयोग करते हैं। एक विशेष कैरेक्टर सेट का उपयोग डेटा को स्वरूपित करने और लिंक के पार सूचना के हस्तांतरण की निगरानी के लिए किया जाता है। विभिन्न चरित्र कोड विकसित किए गए हैं। उपयोग किए गए बिट्स की संख्या से ये कैरेक्टर कोड लंबाई में भिन्न होते हैं। ग्राफिक्स कैरेक्टर हैं, जो प्रतीकों, नियंत्रण कैरेक्टर का प्रतिनिधित्व करते हैं, जिनका उपयोग रिमोट टर्मिनल और संचार कैरेक्टर को नियंत्रित करने के लिए किया जाता है, जो कम्प्यूटर कार्यों जैसे कि सिंक्रनाइजेशन और संदेश हैंडलिंग को नियंत्रित करते हैं।

सबसे आम कैरेक्टर–उन्मुख कोड सात–बिट ASCII कोड है। ASCII का अर्थ सूचना मानक के लिए अमेरिकन स्टैंडर्ड कोड है। प्रत्येक कैरेक्टर की पहचान 7–बिट बाइनरी कोड के माध्यम से की जाती है। त्रुटि का पता लगाने के उद्देश्य से एक अतिरिक्त बिट जोड़ा जाता है। इस बिट को समता बिट के रूप में जाना जाता है। प्रत्येक कैरेक्टर में 1's की संख्या इस बिट को निर्धारित करती है। यदि बिट्स की संख्या सम है, तो बिट्स की कुल संख्या को विषम बनाने के लिए, 1 बिट का उपयोग समता बिट के रूप में किया जाता है। इस प्रक्रिया को विषम समता के रूप में जाना जाता है। समता के साथ, यदि कैरेक्टर में 1's की संख्या विषम है, तो सम संख्या में 1's की कुल संख्या बनाने के लिए, समता बिट के रूप में एक 1 बिट जोड़ा जाता है, अन्यथा एक समता बिट के रूप में उपयोग किया जाता है। एक अन्य व्यापक रूप से इस्तेमाल किया जाने वाला कैरेक्टर कोड विस्तारित बाइनरी कोडेड दशमलव इंटरचेंज कोड (EBCDIC) है। यह ASCII कोड के समान एक आठ–बिट कोड है।

भले ही कैरेक्टर–उन्मुख प्रोटोकॉल कई अनुप्रयोगों में बड़े पैमाने पर उपयोग किए जाते हैं, उनके पास कमियों की संख्या है। इस वजह से, वे शायद ही कभी आधुनिक अनुप्रयोगों में उपयोग किए जाते हैं।

2. बिट–उन्मुख प्रोटोकॉलः

कई बिट–उन्मुख प्रोटोकॉल में से, कुछ महत्वपूर्ण प्रोटोकॉल और उन्हें विकसित करने वाले संगठन नीचे दिए गए हैं।

- उच्च स्तरीय डेटा लिंक कंट्रोल (HDLC) – अंतर्राष्ट्रीय मानक संगठन।
- उन्नत डेटा संचार नियंत्रण प्रक्रिया (ADCCP) – अमेरिकी राष्ट्रीय मानक संस्थान (ANSI)
- सिंक्रोनस डेटा लिंक कंट्रोल (SDLC) – आईबीएम

HDLC प्रोटोकॉल विशेषताएं:

HDLC प्रोटोकॉल की विशेषताएं निम्नलिखित हैं:

- प्रोटोकॉल और डेटा पूरी तरह से स्वतंत्र हैं। इस गुण को पारदर्शिता के रूप में जाना जाता है।
- यह विभिन्न विन्यास वाले नेटवर्क के लिए उपयुक्त है। उदाहरणों में बिंदु से बिंदु, मल्टी ड्रॉप और लूप कॉन्फिगरेशन सम्मिलित हैं।
- यह अर्द्ध और पूर्ण डुप्लेक्स संचालन का समर्थन करता है।
- यह कुशलता से लंबे समय तक प्रसार में देरी और उच्च डेटा दरों के साथ लिंक पर काम करता है।
- यह उच्च विश्वसनीयता प्रदान करता है। डेटा हानि, डेटा दोहराव और डेटा भ्रष्टाचार जैसी समस्याएं उत्पन्न नहीं होती हैं।

HDLC प्रोटोकॉल:

HDLC प्रोटोकॉल के लिए ऑपरेशन के तीन तरीके परिभाषित किए गए हैं। वो हैं:

- सामान्य प्रतिक्रिया मोड (NRM)
- एसिंक्रोनस रिस्पांस मोड (ARM)
- एसिंक्रोनस बैलेंस्ड मोड (ABM)

पहले दो मोड बिंदु से बिंदु और मल्टी ड्रॉप कॉन्फिगरेशन के लिए उपयोगी हैं। इन दो मोड्स में, एक प्राथमिक स्टेशन और एक या अधिक माध्यमिक स्टेशन हैं। प्राथमिक स्टेशन लिंक के प्रारंभिककरण के लिए उत्तरदायी है, प्राथमिक और माध्यमिक स्टेशन्स, त्रुटि नियंत्रण के मध्य डेटा प्रवाह को नियंत्रित करता है, और माध्यमिक स्टेशन्स का तार्किक वियोग।

NRM मोड में, प्राथमिक स्टेशन, माध्यमिक स्टेशन्स को प्रसारण शुरू करने की अनुमति देने से पहले, मतदान करता है। लेकिन ARM मोड में, माध्यमिक स्टेशन बिना मतदान के प्रसारण शुरू कर सकता है। NRM मल्टी ड्रॉप वातावरण के लिए सबसे उपयुक्त है।

ABM मोड केवल बिन्दु–से–बिन्दु कॉन्फिगरेशन के लिए उपयुक्त है। प्रत्येक स्टेशन जरूरत के आधार पर एक प्राथमिक और माध्यमिक की भूमिका निभाता है। इस मोड में कोई मतदान नहीं है। HDLC प्रोटोकॉल में, डेटा फ्रेम के रूप में प्रेषित होता है। फ्रेम में छः फील्ड शामिल हैं। कुछ फील्ड को विस्तार से नीचे समझाया गया है।

फ्लेगः इस फील्ड का उपयोग किसी फ्रेम के प्रारंभ और अंत को इंगित करने के लिए किया जाता है। एक विशेष आठ–बिट अनुक्रम 01111110 को एक फ्लेग के रूप में संदर्भित किया गया है। प्रत्येक फ्रेम एक फ्लेग के साथ आरंभ और समाप्त होता है। चूंकि यह बिट, अनुक्रम सूचना क्षेत्र में डेटा में गलती से हो सकता है, इसलिए उपयोगी डेटा में इस पैटर्न की घटना से बचने के लिए देखभाल की जानी चाहिए। HDLC में, बिट स्टफिंग नामक एक तकनीक यह प्रदर्शन करती है।

एड्रेसः इस फील्ड में द्वितीयक स्टेशन का पता होता है। इस फील्ड में एक या अधिक 8–बिट पते हो सकते हैं। 8–बिट पते का उपयोग तब किया जाता है जब स्टेशन्स की कुल संख्या 256 से अधिक हो जाती है। अन्यथा दो–बाइट पते का उपयोग करते हैं।

नियंत्रण: यह फील्ड फ्रेम के फंक्शन और उद्देश्य की पहचान करता है। प्रोटोकॉल के आधार पर, 8–बिट या 16–बिट नियंत्रण फील्ड का उपयोग किया जाता है।

डेटाः इस फील्ड में प्रेषित किया जाने वाला उपयोगकर्ता डेटा है। यह वांछित ढंग से लंबा या रिक्त हो सकता है।

12.1 डाटा लिंक लेयर (आंकड़ा कड़ी परत) में सुरक्षा:

ईथरनेट नेटवर्क में डेटा लिंक लेयर पर कई हमलों का खतरा है। सबसे आम हमले हैं:

ARP स्पूफिंग:

एड्रेस रिजॉल्यूशन प्रोटोकॉल (ARP) एक ऐसा प्रोटोकॉल है जिसका उपयोग स्थानीय ईथरनेट में पहचाने जाने वाले भौतिक मशीन के पते के लिए एक IP पते को मैप करने के लिए किया जाता है। जब एक होस्ट मशीन को एक IP पते के लिए भौतिक मीडिया एक्सेस कंट्रोल (MAC) पता खोजने की आवश्यकता होती है, तो यह ARP अनुरोध को प्रसारित करता है। अन्य होस्ट जो IP पते का मालिक है, अपने भौतिक पते के साथ ARP उत्तर संदेश भेजता है।

नेटवर्क पर प्रत्येक होस्ट मशीन एक तालिका रखता है, जिसे ARP कैश कहा जाता है। तालिका IP पता और नेटवर्क पर अन्य होस्ट के MAC पते रखता है।

चूँकि ARP एक स्टेटलेस प्रोटोकॉल होता है, हर बार एक होस्ट को दूसरे होस्ट से ARP उत्तर मिलता है, भले ही उसने ARP प्रार्थना न भेजी हो, लेकिन वह ARP एंट्री स्वीकार करता है और अपने ARP कैश को अद्यतन करता है। ARP पॉइजनिंग या ARP स्पूफिंग नामक जाली प्रविष्टि के साथ एक लक्ष्य होस्ट के ARP कैश को संशोधित करने की प्रक्रिया।

ARP स्पूफिंग एक हमलावर को वैध होस्ट के रूप में बहकने की अनुमति दे सकती है और फिर एक नेटवर्क पर डेटा फ्रेम को रोक सकती है, उन्हें संशोधित या रोक सकती है। अक्सर हमले का उपयोग अन्य हमलों जैसे कि मानव–मध्य, सत्र अपहरण, या सेवा से वंचित करने के लिए किया जाता है।

MAC फ्लडिंग:

ईथरनेट में प्रत्येक स्विच में एक सामग्री–पता योग्य मेमोरी (CAM) तालिका होती है जो MAC पते, स्विच पोर्ट नंबर और अन्य जानकारी संग्रहीत करती है। तालिका का एक निश्चित आकार है। MAC फ्लड हमले में, CAM तालिका भरे होने तक जाली ARP पैकेट का उपयोग करके MAC पते के साथ हमलावर स्विच पर हमला कर देता है।

एक बार CAM भर जाने के बाद, स्विच हब–जैसे मोड में चला जाता है और वह ट्रैफिक प्रसारित करना शुरू कर देता है जिसमें CAM प्रविष्टि नहीं है। हमलावर जो एक ही नेटवर्क पर है, अब उन सभी फ्रेम्स को प्राप्त करता है जो केवल एक विशिष्ट होस्ट के लिए थे।

पोर्ट चोरी:

ईथरनेट स्विच में पोर्ट के MAC एड्रेस को सीखने और बांधने की क्षमता होती है। जब एक स्विच MAC स्रोत पते के साथ एक पोर्ट से ट्रैफिक प्राप्त करता है, तो यह पोर्ट नंबर और उस MAC पते को बांधता है।

पोर्ट चोरी हमले स्विच की इस क्षमता का फायदा उठाते हैं। हमलावर स्रोत के रूप में लक्ष्य होस्ट के MAC पते के साथ जाली ARP फ्रेम के साथ स्विच को फ्लड कर देता है। स्विच को यह विश्वास करने के लिए मूर्ख बनाया जाता है कि लक्ष्य होस्ट पोर्ट पर है, जिस पर वास्तव में एक हमलावर जुड़ा हुआ है।

अब लक्षित होस्ट के लिए इच्छित सभी डेटा फ्रेम हमलावर के स्विच पोर्ट पर भेजे जाते हैं और लक्ष्य होस्ट पर नहीं। इस प्रकार, हमलावर अब उन सभी फ्रेम्स को प्राप्त करता है जो वास्तव में केवल लक्ष्य होस्ट के लिए नियत किए गए थे।

DHCP हमले:

डायनामिक होस्ट कॉन्फिगरेशन प्रोटोकॉल (DHCP) एक डॉटलिंक प्रोटोकॉल नहीं है लेकिन DHCP हमलों के समाधान लेयर 2 हमलों को विफल करने के लिए भी उपयोगी हैं।

DHCP का उपयोग विशिष्ट समय अवधि के लिए कम्प्यूटर पर IP पते को गतिशील रूप से आबंटित करने के लिए किया जाता है। नेटवर्क में सेवा से वंचित या DHCP सर्वर को लागू करने से DHCP सर्वर पर हमला करना संभव है। एक DHCP पर हमले में, हमलावर सभी उपलब्ध DHCP पते का अनुरोध करता है। यह नेटवर्क पर वैध होस्ट की सेवा से इनकार करता है। डीएचसीपी स्पूफिंग हमले में, क्लाइंट को पते प्रदान करने के लिए हमलावर एक दुष्ट DHCP सर्वर को तैनात कर सकता है।

यहाँ, हमलावर DHCP प्रतिक्रियाओं के साथ एक डिफॉल्ट गेटवे के साथ मेजबान मशीनें प्रदान कर सकता है। होस्ट से डेटा फ्रेम अब गेटवे को लाल करने के लिए निर्देशित किए जाते हैं जहाँ हमलावर सभी पैकेज को रोक सकता है और वास्तविक गेटवे का जवाब दे सकता है या उन्हें ड्रॉप कर सकता है।

अन्य हमलेः

उपरोक्त लोकप्रिय हमलों के अतिरिक्त, अन्य हमले भी हैं जैसे लेयर 2–आधारित प्रसारण, डेनियल ऑफ सर्विस (DOS), MAC क्लोनिंग।

प्रसारण हमले में, हमलावर नेटवर्क पर मेजबान को खराब ARP जवाब भेजता है। ये ARP उत्तर डिफॉल्ट गेटवे के MAC पते को प्रसारण पते पर सेट करते हैं। यह सभी आउटबाउंड ट्रैफिक को प्रसारित करने का कारण बनता है, एक ही ईथरनेट पर बैठे हमलावर द्वारा सूँघने को सक्षम करता है। इस तरह के हमले से नेटवर्क क्षमता भी प्रभावित होती है।

लेयर 2–आधारित DOS हमलों में, हमलावर गैर–मौजूद MAC पते के साथ नेटवर्क में होस्ट के ARP कैश को अपडेट करता है। किसी नेटवर्क में प्रत्येक नेटवर्क इंटरफेस कार्ड का MAC पता विश्व स्तर पर अद्वितीय माना जाता है। हालांकि, MAC क्लोनिंग को सक्षम करके इसे आसानी से बदला जा सकता है। हमलावर DOS हमले के माध्यम से लक्ष्य होस्ट को निष्क्रिय कर देता है और फिर लक्षित होस्ट के IP और MAC पते का उपयोग करता है।

हमलावर नेटवर्क पर यात्रा करने वाली सूचना की सुरक्षा को खतरे में डालने के लिए उच्च स्तर के हमलों को शुरू करने के लिए हमलों को अंजाम देता है। वह सभी फ्रेम्स को अवरोधित कर सकता है और फ्रेम डेटा को पढ़ने में सक्षम होगा। हमलावर एक मानव–मध्य के रूप में कार्य कर सकता है और डेटा को संशोधित कर सकता है या बस DOS के लिए अग्रणी फ्रेम को गिरा सकता है। वह लक्ष्य होस्ट और अन्य मशीनों के मध्य चल रहे सत्र को हाईजैक कर सकता है, और पूरी तरह से गलत जानकारी का संचार कर सकता है।

12.2 सुरक्षित ईथरनेट लैनः

हमने पिछले अनुच्छेद में डेटा लिंक लेयर पर कुछ व्यापक रूप से ज्ञात हमलों पर चर्चा की। इस प्रकार के हमलों को कम करने के लिए कई विधियाँ विकसित की गई हैं। कुछ महत्वपूर्ण विधियाँ हैंः

पोर्ट सुरक्षाः

यह ईथरनेट स्विच पर उपलब्ध एक परत 2 सुरक्षा सुविधा है। इसमें एक स्विच के भौतिक पोर्ट को एक विशिष्ट MAC पते में बांधना शामिल है। उपलब्ध स्विच पोर्ट में से किसी एक को होस्ट कनेक्ट करके कोई भी असुरक्षित नेटवर्क तक पहुंच सकता है। लेकिन, पोर्ट सिक्योरिटी लेयर 2 एक्सेस को सुरक्षित कर सकती है।

डिफॉल्ट रूप से, पोर्ट सुरक्षा एक के लिए MAC पता गिनती को सीमित करती है। हालांकि, कॉन्फिगरेशन के माध्यम से उस पोर्ट से कनेक्ट करने के लिए एक से अधिक अधिकृत होस्ट की अनुमति देना संभव है। प्रति इंटरफेस में अनुमत MAC पते को सांख्यिकीय रूप से कॉन्फिगर किया जा सकता है। एक सुविधाजनक विकल्प अस्थिर MAC पते को सक्षम करना है जहाँ MAC पते गतिशील रूप से स्विच पोर्ट द्वारा सीखे जाएंगे जब तक कि पोर्ट के लिए अधिकतम सीमा नहीं पहुँच जाती है।

सुरक्षा सुनिश्चित करने के लिए, निर्दिष्ट MAC पते में परिवर्तन की प्रतिक्रिया/पोर्ट पर या पोर्ट पर अतिरिक्त पते को कई अलग–अलग विधियों से नियंत्रित किया जा सकता है। पोर्ट को एक सीमित सीमा से अधिक MAC पते को बंद करने या ब्लॉक करने के लिए कॉन्फिगर किया जा सकता है। पोर्ट को बंद करने के लिए अनुशंसित सर्वोत्तम अभ्यास है। पोर्ट सुरक्षा MAC फ्लड और क्लोनिंग हमलों को रोकता है।

DHCP स्नूपिंगः

हमने देखा है कि DHCP स्पूफिंग एक हमला है जहाँ हमलावर नेटवर्क पर होस्ट से DHCP के अनुरोधों को सुनता है और अधिकृत DHCP प्रतिक्रिया के होस्ट के आने से पहले नकली DHCP प्रतिक्रिया के साथ उनका जवाब देता है।

DHCP स्नूपिंग ऐसे हमलों को रोक सकता है। DHCP स्नूपिंग एक स्विच लक्षण है। स्विच को यह निर्धारित करने के लिए कॉन्फिगर किया जा सकता है कि कौन से स्विच पोर्ट DHCP के अनुरोधों का जवाब दे सकते हैं। स्विच पोर्ट को विश्वसनीय या अविश्वसनीय पोर्ट के रूप में पहचाना जाता है।

केवल एक अधिकृत DHCP सर्वर से कनेक्ट होने वाले पोर्ट को विश्वसनीय के रूप में कॉन्फिगर किया गया है, और सभी प्रकार के DHCP संदेशों को भेजने की अनुमति है। स्विच पर अन्य सभी पोर्ट अविश्वसनीय हैं और केवल DHCP अनुरोध भेज सकते हैं। यदि एक अविश्वसनीय पोर्ट पर DHCP प्रतिक्रिया देखी जाती है, तो पोर्ट बंद हो जाता है।

ARP स्पूफिंग को रोकनाः

पोर्ट सुरक्षा की विधि MAC फ्लड और क्लोनिंग हमलों को रोक सकती है। हालांकि, यह ARP स्पूफिंग को नहीं रोकता है। पोर्ट सुरक्षा फ्रेम हेडर में MAC स्रोत पते को मान्य करता है, लेकिन ARP फ्रेम में डेटा पेलोड में एक अतिरिक्त MAC स्रोत फील्ड होता है, और होस्ट अपने ARP कैश को बढ़ाने के लिए इस फील्ड का उपयोग करता है। ARP स्पूफिंग को रोकने के लिए कुछ विधियाँ निम्नानुसार सूचीबद्ध हैं।

स्थैतिक ARP: अनुशंसित कार्रवाई में से एक होस्ट ARP तालिका में स्थिर ARP प्रविष्टियों को नियोजित करना है। स्थैतिक ARP प्रविष्टियाँ ARP कैश में स्थायी प्रविष्टियाँ हैं। हालाँकि, यह विधि अव्यवहारिक है। इसके अतिरिक्त, यह कुछ डायनामिक होस्ट कॉन्फिगरेशन प्रोटोकॉल (DHCP) के उपयोग की अनुमति नहीं देता है क्योंकि लेयर 2 नेटवर्क में सभी होस्ट के लिए स्थिर IP का उपयोग करने की आवश्यकता होती है।

घुसपैठ का पता लगाने की प्रणालीः रक्षा की विधि ARP यातायात की उच्च मात्रा का पता लगाने के लिए कॉन्फिगर की गई घुसपैठ परीक्षण प्रणाली (IDS) का उपयोग करना है। हालांकि, IDS झूठी सकारात्मक रिपोर्ट करने के लिए प्रवण है।

गतिक एआरपी निरीक्षणः ARP स्पूफिंग को रोकने की यह विधि DHCP स्नूपिंग के समान है। यह विश्वसनीय और अविश्वसनीय पोर्ट का उपयोग करता है। ARP उत्तरों को केवल विश्वसनीय पोर्ट पर स्विच इंटरफेस में अनुमति दी जाती है। यदि कोई ARP उत्तर किसी अविश्वसनीय पोर्ट पर स्विच करने के लिए आता है, तो ARP उत्तर पैकेट की सामग्री की तुलना इसकी शुद्धता को सत्यापित करने के लिए DHCP बाइंडिंग तालिका से की जाती है। यदि ARP उत्तर मान्य नहीं है, तो ARP उत्तर छोड़ दिया जाता है, और पोर्ट अक्षम हो जाता है।

12.3 सुरक्षित स्पानिंग ट्री प्रोटोकॉल (सुरक्षित विस्तरित तरू संदेशाचार):

स्पैनिंग ट्री प्रोटोकॉल (STP) एक परत 2 लिंक प्रबंधन प्रोटोकॉल है। STP का मुख्य उद्देश्य यह सुनिश्चित करना है कि नेटवर्क के बेमानी रास्ते होने पर कोई डेटा फ्लो लूप न हो। आमतौर पर, नेटवर्क को विश्वसनीयता प्रदान करने के लिए निरर्थक रास्ते बनाए जाते हैं। लेकिन वे घातक छोरों का निर्माण कर सकते हैं जो नेटवर्क में DOS हमले का कारण बन सकते हैं।

स्पेनिंग ट्री प्रोटोकॉलः

वांछित पथ अतिरेक प्रदान करने के लिए, साथ ही एक लूप स्थिति से बचने के लिए, STP एक पेड़ को परिभाषित करता है जो एक नेटवर्क में सभी स्विच को फैलाता है। STP कुछ अनावश्यक डेटा लिंक को अवरुद्ध अवस्था में ले जाता है और अन्य लिंक को अग्रेषित स्थिति में रखता है।

यदि अग्रेषण स्थिति में एक लिंक टूट जाता है, तो STP नेटवर्क को पुनः कॉन्फिगर करता है और उचित स्टैंडबाय पथ को सक्रिय करके डेटा पथ को फिर से परिभाषित करता है। एसटीपी नेटवर्क में तैनात पुलों और स्विच पर चलता है। सभी स्विच रूट स्विच चयन के लिए और नेटवर्क के बाद के कॉन्फिगरेशन के लिए सूचना का आदान–प्रदान करते हैं। ब्रिज प्रोटोकॉल डेटा यूनिट्स (BPDU) इसकी जानकारी लेती हैं। BPDU के आदान–प्रदान के माध्यम से, नेटवर्क के सभी स्विच रूट ब्रिज/स्विच का चुनाव करते हैं जो नेटवर्क में फोकल पॉइंट बन जाता है और अवरुद्ध और अग्रेषित लिंक को नियंत्रित करता है।

STP पर हमलेः

- रूट ब्रिज पर ले जानाः यह परत 2 पर सबसे विघटनकारी प्रकार का हमला है। डिफॉल्ट रूप से, एक लैन स्विच किसी भी BPDU को पड़ोसी स्विच से अंकित मूल्य पर भेजा जाता है। संयोग से, STP विश्वसनीय, स्टेटलेस है, और कोई ध्वनि प्रमाणीकरण तंत्र प्रदान नहीं करता है।
- रूट अटैक मोड में एक बार, हमलावर स्विच वर्तमान रूट ब्रिज की तरह ही प्राथमिकता के साथ हर 2 सेकंड में एक BPDU भेजता है, लेकिन थोड़े संख्यात्मक रूप से कम MAC पते के साथ, जो रूट–ब्रिज चुनाव प्रक्रिया में अपनी जीत सुनिश्चित करता है। हमलावर स्विच या तो BPDU फ्लड के कारण अन्य स्विच को ठीक से स्वीकार न करके या एक समय में रूट होने का दावा करके BPDU पर स्विच करने और त्वरित उत्तराधिकार में पीछे हटने से DOS हमले का शुभारंभ कर सकता है।
- विन्यास BPDU के फ्लड का उपयोग करते हुए। आक्रमण स्विच जड़ के रूप में लेने की कोशिश नहीं करता है। इसके बजाय, यह स्विच पर बहुत अधिक CPU उपयोग के लिए प्रति सेकंड बड़ी संख्या में BPDUs उत्पन्न करता है।

STP पर हमलों को रोकनाः

सौभाग्य से, रूट टेकओवर हमले का प्रतिवाद सरल और सीधा है। दो विशेषताएं रूट टेकओवर हमले को हराने में सहायता करती हैं।

रूट गार्डः रूट गार्ड स्विच पोर्ट को प्रतिबंधित करता है जिसमें से रूट ब्रिज पर बातचीत की जा सकती है। यदि कोई DU रूट–गार्ड–सक्षम 'पोर्ट BPDUs प्राप्त करता है जो उन लोगों के लिए बेहतर है जो वर्तमान रूट ब्रिज भेज रहे हैं, तो उस पोर्ट को रूट–असंगत स्थिति में ले जाया जाता है, और उस पोर्ट पर कोई डेटा ट्रैफिक अग्रेषित नहीं किया जाता है। रूट गार्ड को उन पोर्ट्स की ओर सर्वोत्तम रूप से तैनात किया जाता है जो स्विच से जुड़ते हैं जो रूट ब्रिज के रूप में कार्यभार संभालने की उम्मीद नहीं करते हैं।

BPDU गार्डः BPDU गार्ड का उपयोग उन नेटवर्क की समस्याओं से बचाने के लिए किया जाता है जो एक्सेस पोर्ट पर BPDU की प्राप्ति के कारण हो सकते हैं। ये ऐसे पोर्ट हैं जो उन्हें प्राप्त नहीं होने चाहिए। BPDU गार्ड को एक हमलावर द्वारा दुष्ट स्विच की प्रविष्टि को रोकने के लिए उपयोगकर्ता सामना करने वाले पोर्ट्स की ओर सबसे अच्छा तैनात किया गया है।

एसटीपी स्विच पोर्ट अवस्थाः

LAN में सभी स्विच पोर्ट जहाँ STP सक्षम है, श्रेणीबद्ध हैं।

ब्लॉकिंगः

एक पोर्ट जो सक्रिय होने पर स्विचिंग लूप का कारण होगा। कोई उपयोगकर्ता डेटा अवरुद्ध पोर्ट पर नहीं भेजा या प्राप्त किया जाता है, लेकिन यह अग्रेषण मोड में जा सकता है यदि उपयोग में अन्य लिंक विफल हो जाते हैं और स्पानिंग ट्री एल्गोरिथ्म निर्धारित करते हैं कि पोर्ट अग्रेषण स्थिति में संक्रमण कर सकता है। BPDU डेटा अभी भी अवरुद्ध अवस्था में प्राप्त होता है। लूप पथों के उपयोग को रोकता है।

सुननाः

स्विच BPDUs को संसाधित करता है और संभावित नई जानकारी की प्रतीक्षा करता है जिससे यह अवरुद्ध स्थिति में वापस आ जाएगा। यह मैक एड्रेस टेबल को नहीं बढ़ाता है और यह फ्रेम को अग्रेषित नहीं करता है।

सीखनाः

हालांकि पोर्ट अभी तक फ्रेम को अग्रेषित नहीं करता है, यह प्राप्त फ्रेम से स्रोत पते सीखता है और उन्हें फिल्टरिंग डेटाबेस (स्विचिंग डेटाबेस) में जोड़ता है। यह MAC एड्रेस तालिका को बढ़ाता है, लेकिन फ्रेम को अग्रेषित नहीं करता है।

अग्रेषित करनाः

ईथरनेट फ्रेम, सामान्य संक्रिया में डेटा प्राप्त करने और भेजने वाला पोर्ट। अग्रेषण पोर्ट आने वाले BPDU को मॉनिटर करता है जो यह दर्शाता है कि लूप को रोकने के लिए इसे अवरुद्ध स्थिति में वापस आना चाहिए।

असमर्थः

एक नेटवर्क व्यवस्थापक ने मैन्युअल रूप से एक स्विच पोर्ट को अक्षम कर दिया है।

जब कोई डिवाइस प्रथम बार एक स्विच पोर्ट से जुड़ा होता है, तो यह तुरंत अग्रेषित डेटा को आरंभ नहीं करेगा। इसके स्थान पर यह कई अवस्थाओं से गुजरेगा जबकि यह BPDU को संसाधित करता है और नेटवर्क की टोपोलॉजी को निर्धारित करता है। जब कोई होस्ट संलग्न होता है, जैसे कि कम्प्यूटर, प्रिंटर या सर्वर, तो पोर्ट हमेशा अग्रेषित स्थिति में चला जाता है, यद्यपि यह लगभग 30 सेकंड की देरी के बाद होता है जबकि यह सुनने और सीखने की अवस्थाओं से गुजरता है। सुनने और सीखने की अवस्था में बिताए गए समय को एक मान के रूप में जाना जाता है जिसे आगे की देरी (मूल 15 सेकंड और रूट ब्रिज द्वारा व्यवस्थित) के रूप में जाना जाता है। हालांकि, अगर इसके स्थान पर एक और स्विच जुड़ा हुआ है, तो पोर्ट अवरुद्ध मोड में रह सकता है, यदि यह निर्धारित किया जाता है कि यह नेटवर्क में एक लूप का कारण होगा। टोपोलॉजी चेंज नोटिफिकेशन (Topology Change Notification - TCN) BPDU का उपयोग पोर्ट परिवर्तन के अन्य स्विच को सूचित करने के लिए किया जाता है। TCN को एक गैर–रूट स्विच द्वारा नेटवर्क में इंजेक्ट किया जाता है और रूट को प्रचारित किया जाता है। TCN प्राप्त होने पर, रूट स्विच अपने सामान्य BPDU में टोपोलॉजी चेंज फ्लैग व्यवस्थित करेगा। इस फ्लैग को अन्य सभी स्विच्स के लिए प्रचारित किया जाता है ताकि वे अपनी अग्रेषण तालिका प्रविष्टियों को तेजी से दे सकें।

हानिः

स्पानिंग ट्री एक पुराना प्रोटोकॉल है जिसमें एक लंबे समय तक डिफॉल्ट होल्ड–डाउन समय होता है जो प्रोटोकॉल अवस्था के अभिसरण को नियंत्रित करता है। अनुचित उपयोग या कार्यान्वयन नेटवर्क अवरोधों में योगदान कर सकते हैं। लिंक अवरुद्ध करने का विचार कुछ ऐसा है जो क्लाइंट इन दिनों उचित उच्च उपलब्धता समाधान के रूप में स्वीकार नहीं करते हैं।

मुख्य रूप से नेटवर्क टोपोलॉजी लूप का प्रबंधन करने के लिए एक गार्ड प्रोटोकॉल के रूप में डिजाइन किए जाने के बाद भी, स्पैनिंग ट्री प्रोटोकॉल का अक्सर उच्च–उपलब्धता विधि के रूप में दुरुपयोग किया गया था। आधुनिक नेटवर्क डिजाइन में आमतौर पर नेटवर्क मीडिया और डिवाइस संक्रिया को समझने में कमी होती है जिसके परिणामस्वरूप होता है, टोपोलॉजी लूप्स, चाहे वह भौतिक हो या तार्किक। आधुनिक नेटवर्क सभी कनेक्टेड लिंक का उपयोग प्रोटोकॉल के उपयोग से कर सकते हैं जो तार्किक या भौतिक टोपोलॉजी लूप के प्राकृतिक व्यवहार को रोकते, नियंत्रित या दबाते हैं।

HPE IRF, Aruba VSF और Cisco VSS जैसी वर्चुअलाइजेशन तकनीकों को एक तार्किक इकाई में कई स्विच जोड़ते हैं। एक मल्टी–चेसिस लिंक एग्रीगेशन ग्रुप एक सामान्य LACP ट्रंक के समान कार्य करता है, जो केवल कई स्विच के माध्यम से वितरित किया जाता है। इसके विपरीत विभाजन प्रौद्योगिकियाँ एक एकल भौतिक चेसिस को कई तार्किक संस्थाओं में संकलित करती हैं।

नेटवर्क के किनारे पर, उपयोगकर्ताओं द्वारा आकस्मिक लूप को रोकने के लिए लूप–डिटेक्शन कॉन्फिगर किया गया है।

12.4 सुरक्षित आभासी लैनः

स्थानीय नेटवर्क में, वर्चुअल लोकल एरिया नेटवर्क (Virtual Local Area Networks - VLAN) को कभी–कभी हमलों की परत 2 के लिए अतिसंवेदनशील होस्ट्स की संख्या को सीमित करने के लिए एक सुरक्षा उपाय के रूप में कॉन्फिगर किया जाता है। VLAN नेटवर्क सीमाएँ बनाते हैं, जिनके ऊपर प्रसारण (ARP, DHCP) यातायात पार नहीं कर सकता है।

वर्चुअल लोकल एरिया नेटवर्कः

VLAN क्षमताओं का समर्थन करने वाले स्विच को नियोजित करने वाले नेटवर्क को एक ही भौतिक LAN बुनियादी ढांचे पर कई VLAN को परिभाषित करने के लिए कॉन्फिगर किया जा सकता है। VLAN का सामान्य रूप पोर्ट–आधारित VLAN है। इस VLAN संरचना में, स्विच प्रबंधन सॉफ्टवेयर का उपयोग करके स्विच पोर्ट को VLAN में वर्गीकृत किया जाता है। इस प्रकार एक एकल भौतिक स्विच कई आभासी स्विच के रूप में कार्य कर सकता है।

VLAN के नियोजन यातायात अलगाव प्रदान करते हैं। यह बड़ी प्रसारण परत 2 नेटवर्क को छोटे तार्किक परत 2 नेटवर्क में विभाजित करता है और इस प्रकार ARP/DHCP स्पूफिंग जैसे हमलों की सीमा को कम करता है। एक VLAN के डेटा फ्रेम केवल उसी VLAN से संबंधित पोर्ट्स के अंदर से/को आगे बढ़ सकते हैं। दो VLAN के मध्य अग्रेषण करने वाले फ्रेम को रूटिंग के माध्यम से किया जाता है।

VLAN आमतौर पर कई स्विचों को फैलाते हैं। ट्रंक पोर्ट के मध्य लिंक कई भौतिक स्विच्स पर परिभाषित सभी VLAN के फ्रेम ले जाता है। इसलिए, स्विच के मध्य अग्रेषित VLAN फ्रेम साधारण IEEE 802.1 ईथरनेट प्रारूप फ्रेम नहीं हो सकते। चूंकि, ये फ्रेम उसी भौतिक लिंक पर चलते हैं, इसलिए उन्हें अब VLAN ID जानकारी ले जाने की आवश्यकता है। IEEE 802.1Q प्रोटोकॉल ट्रंक पोर्ट्स के मध्य प्लेन ईथरनेट फ्रेम्स में अतिरिक्त हेडर फील्ड्स को जोड़ता/हटाता है।

जब दो IP पते फील्ड का अनुसरण करने वाला फील्ड 0x8100 (> 1500) है, तो फ्रेम को 802.1Q फ्रेम के रूप में पहचाना जाता है। 2–बाइट टैग प्रोटोकॉल आइडेंटिफायर (TPI) का मान 81–00 है। TCI क्षेत्र में 3–बिट प्राथमिकता की जानकारी, 1–बिट ड्रॉप इलिजबिल इंडिकेटर (DEI), और 12–बिट VLAN ID सम्मिलित हैं। यह 3–बिट प्राथमिकता क्षेत्र और DEI फील्ड VLAN के लिए प्रासंगिक नहीं है। गुणवत्ता की सेवा के प्रावधान के लिए प्राथमिकता बिट्स का उपयोग किया जाता है।

जब कोई फ्रेम किसी VLAN से संबंधित नहीं होता है, तो एक डिफॉल्ट VLAN ID होता है जिसे फ्रेम के साथ जुड़ा हुआ माना जाता है।

एक वर्चुअल LAN (VLAN) किसी भी ब्रॉडकास्ट डोमेन का है जो डेटा लिंक लेयर (OSI परत 2) में एक कम्प्यूटर नेटवर्क में विभाजित और पृथक किया जाता है। LAN स्थानीय क्षेत्र नेटवर्क का संक्षिप्त नाम है और इस संदर्भ में आभासी एक भौतिक वस्तु को संदर्भित करता है जिसे अतिरिक्त तर्क द्वारा पुनः निर्मित और परिवर्तित किया जाता है।

VLAN नेटवर्क फ्रेम में टैग लगाकर और नेटवर्किंग सिस्टम में इन टैग को संभालकर काम करते हैं – नेटवर्क ट्रैफिक की उपस्थिति और कार्यक्षमता का निर्माण जो शारीरिक रूप से एकल नेटवर्क पर होता है, लेकिन यह कार्य करता है जैसे कि यह पृथक नेटवर्क के मध्य विभाजित होता है। इस प्रकार, VLAN एक ही भौतिक नेटवर्क से जुड़े होने के उपरान्त भी नेटवर्क अनुप्रयोगों को अलग रख सकता है, और बिना केबल बिछाने और नेटवर्किंग उपकरणों के कई समूह की आवश्यकता के बिना तैनात किया जा सकता है।

VLAN नेटवर्क प्रशासकों को एक साथ होस्ट करने की अनुमति देता है, भले ही होस्ट सीधे एक ही नेटवर्क स्विच से कनेक्ट न हों। क्योंकि VLAN सदस्यता को सॉफ्टवेयर के माध्यम से कॉन्फिगर किया जा सकता है, यह नेटवर्क डिजाइन और परिनियोजन को सरल बना सकता है। VLAN के बिना, होस्ट को अपने संसाधन के अनुसार समूहबद्ध करने के लिए नोड्स को स्थानांतरित करने या डेटा लिंक को पुनः स्थापित करने के श्रम की आवश्यकता होती है। VLAN नेटवर्क और उपकरणों को अनुमति देता है, जिन्हें बिना बातचीत के, समानता, सुरक्षा, यातायात प्रबंधन, या अर्थव्यवस्था में सुधार के बिना एक ही भौतिक केबल को साझा करने के लिए पृथक रखा जाना चाहिए। उदाहरण के लिए, एक VLAN का उपयोग उपयोगकर्ताओं के कारण किसी व्यवसाय के भीतर ट्रैफिक को अलग करने के लिए और नेटवर्क व्यवस्थापकों के मध्य या ट्रैफिक के प्रकारों के कारण किया जा सकता है, ताकि उपयोगकर्ता या कम प्राथमिकता वाला ट्रैफिक नेटवर्क के शेष कार्यों को सीधे प्रभावित न कर सके। कई इंटरनेट होस्टिंग सेवाएं अपने क्लाइंट के व्यक्तिगत जोन को एक–दूसरे से पृथक करने के लिए VLAN का उपयोग करती हैं, जिससे प्रत्येक क्लाइंट के सर्वर को अपने डेटा सेंटर में कहीं भी स्थित होने पर एकल नेटवर्क सेगमेंट में एक साथ समूहीकृत किया जा सकता है। किसी दिए गए VLAN से ट्रैफिक भागने को रोकने के लिए कुछ सावधानियों की आवश्यकता है, एक शोषण जिसे VLAN होपिंग कहा जाता है।

एक नेटवर्क को VLAN में उप–विभाजित करने के लिए, एक नेटवर्क उपकरण को कॉन्फिगर करता है। सरल उपकरण केवल भौतिक पोर्ट (यदि सभी पर) के अनुसार विभाजन कर सकते हैं, तो प्रत्येक दशा में प्रत्येक VLAN एक समर्पित नेटवर्क केबल के साथ जुड़ा हुआ है। अधिक परिष्कृत उपकरण VLAN टैगिंग के माध्यम से फ्रेम को चिह्नित कर सकते हैं, ताकि एक से अधिक आंतरिक संयोजन (ट्रंक) का उपयोग कई VLAN के लिए डेटा परिवहन हेतु किया जा सके। चूंकि VLANs बैंडविड्थ को साझा करते हैं, एक VLAN ट्रंक लिंक एकत्रीकरण, गुणवत्ता–की–सेवा प्राथमिकता, या डेटा को कुशलतापूर्वक रूट करने के लिए दोनों का उपयोग कर सकता है।

उपयोगः

सेवा की खोज, पता असाइनमेंट और रिज़ॉल्यूशन और अन्य सेवाओं के लिए प्रसारण का उपयोग करने वाले नेटवर्क में, चूंकि नेटवर्क पर साथियों की संख्या बढ़ती है, प्रसारण की आवृत्ति भी बढ़ जाती है। VLAN कई प्रसारण डोमेन बनाकर प्रसारण यातायात का प्रबंधन करने में मदद कर सकता है। एक बड़े नेटवर्क को छोटे स्वतंत्र खंडों में तोड़ने से प्रसारण ट्रैफिक की मात्रा कम हो जाती है प्रत्येक नेटवर्क डिवाइस और नेटवर्क सेगमेंट को सहन करना पड़ता है। VLAN के मध्य स्विच नेटवर्क ट्रैफिक को खींच नहीं कर सकते हैं, क्योंकि ऐसा करने से VLAN प्रसारण डोमेन की अखंडता का उल्लंघन होगा।

VLAN एकल भौतिक बुनियादी ढांचे पर कई परत 3 नेटवर्क बनाने में सहायता कर सकता है। VLANs डेटा लिंक लेयर (OSI लेयर 2) संरचना हैं, जो इंटरनेट प्रोटोकॉल (IP) सबनेट्स के अनुरूप हैं, जो नेटवर्क लेयर (OSI लेयर 3) संरचना हैं। VLAN को नियोजित करने वाले वातावरण में, VLAN और IP सबनेट के मध्य एक–से–एक संबंध अक्सर उपलब्ध होता है, हालांकि एक VLAN पर कई सबनेट होना संभव है।

VLAN क्षमता के बिना, उपयोगकर्ताओं को भूगोल पर आधारित नेटवर्क को सौंपा गया है और भौतिक टोपोलॉजी और दूरियों द्वारा सीमित है। VLAN उपयोगकर्ताओं के नेटवर्क स्थान को उनके भौतिक स्थान से हटाने के लिए तार्किक रूप से समूह नेटवर्क बना सकता है। VLAN का उपयोग करके, ट्रैफिक पैटर्न को नियंत्रित किया जा सकता है और कर्मचारी या उपकरण स्थानांतरण के लिए जल्दी से प्रतिक्रिया कर सकता है। VLAN नेटवर्क आवश्यकताओं में बदलाव के लिए अनुकूलता प्रदान करते हैं और सरलीकृत प्रशासन की अनुमति देते हैं।

VLAN का उपयोग स्थानीय नेटवर्क को कई विशिष्ट खंडों में विभाजित करने के लिए किया जा सकता है, उदाहरण के लिएः

- उत्पादन
- IP पर आवाज
- नेटवर्क प्रबंधन
- भंडारण क्षेत्र नेटवर्क (Storage Area Network - SAN)
- अतिथि इंटरनेट पहुँच
- डिमिलिट्राइज्ड जोन (Demilitarized Zone - DMZ)

VLAN और रोकथाम के उपायों पर हमलाः

VLAN होपिंग (Hopping) हमले में, एक VLAN पर एक हमलावर अन्य VLAN पर यातायात तक पहुँच प्राप्त कर सकता है जो सामान्य रूप से सुलभ नहीं होगा। यह एक VLAN से दूसरे में संचार करते समय एक परत 3 डिवाइस (राउटर) को बायपास करेगा, इस प्रकार VLAN निर्माण के उद्देश्य को हरा देगा।

VLAN होपिंग दो तरीकों से किया जा सकता हैः स्विच स्पूफिंग और डबल टैगिंग।

1. स्विचिंग स्पूफिंगः

यह तब हो सकता है जब स्विच पोर्ट, जिसमें हमलावर जुड़ा हुआ है, या तो ट्रंकिंग मोड या ऑटो–वार्ता मोड में है। हमलावर एक स्विच के रूप में कार्य करता है और 802.1Q एनकैप्सुलेशन हेडर को VLAN टैग के साथ लक्षित दूरस्थ VLAN के लिए अपने आउटगोइंग फ्रेम में जोड़ता है। प्राप्त स्विच उन फ्रेस को दूसरे 802.1Q स्विच से छांटता है, और फ्रेम को लक्ष्य VLAN में बदल देता है।

स्विच स्पूफिंग हमलों के विरूद्व दो निवारक उपाय एज पोर्ट्स को स्थैतिक एक्सेस मोड पर सेट करना और सभी पोर्ट्स पर ऑटो–बातचीत को अक्षम करना है।

2. डबल टैगिंगः

इस हमले में, स्विच के देशी VLAN पोर्ट पर जुड़ा एक हमलावर फ्रेम हेडर में दो VLAN टैग प्रस्तुत करता है। पहला टैग मूल VLAN का है और दूसरा लक्ष्य VLAN के लिए है। जब पहले स्विच को हमलावर के फ्रेम मिलते हैं, तो यह पहला टैग हटा देता है क्योंकि मूल VLAN के फ्रेम ट्रंक पोर्ट पर टैग के बिना अग्रेषित किए जाते हैं।

चूंकि पहले स्विच द्वारा दूसरे टैग को कभी हटाया नहीं गया था, इसलिए प्राप्त स्विच शेष टैग को VLAN गंतव्य के रूप में पहचानता है और उस VLAN में लक्ष्य होस्ट के लिए फ्रेम को आगे करता है। डबल टैगिंग हमला मूल VLAN की अवधारणा का शोषण करता है। चूंकि VLAN 1 पहुँच पोर्ट के लिए डिफॉल्ट VLAN और ट्रंक पर डिफॉल्ट मूल VLAN है, इसलिए यह एक आसान लक्ष्य है।

पहला रोकथाम उपाय डिफॉल्ट VLAN 1 से सभी एक्सेस पोर्ट को हटाने के लिए है क्योंकि हमलावर के पोर्ट को स्विच के मूल VLAN से मेल खाना चाहिए। VLAN आईडी 999 को किसी अन्य अप्रयुक्त VLAN के लिए सभी स्विच ट्रंक पर मूल VLAN आबंटित करने के लिए दूसरा रोकथाम उपाय है। और अंत में, सभी स्विच ट्रंक पोर्ट पर मूल VLAN फ्रेम के स्पष्ट टैगिंग को पूरा करने के लिए कॉन्फिगर किए जाएंगे।

12.5 सुरक्षित वायरलेस (बेतार) लैनः

वायरलेस लोकल एरिया नेटवर्क एक सीमित भौगोलिक क्षेत्र के अंदर वायरलेस नोड्स का एक नेटवर्क है, जैसे कि कार्यालय भवन या स्कूल परिसर। नोड्स रेडियो संचार में सक्षम हैं। वायरलेस लैन को आमतौर पर डिवाइस की गतिशीलता के साथ नेटवर्क एक्सेस प्रदान करने के लिए उपलब्ध वायर्ड लैन के एक्सटेंशन के रूप में लागू किया जाता है। सबसे व्यापक रूप से कार्यान्वित वायरलेस लैन तकनीक IEEE 802.11 मानक और उसके संशोधनों पर आधारित हैं।

वायरलेस लैन में दो मुख्य घटक हैंः

एक्सेस पॉइंट्स (APs) – ये वायरलेस नेटवर्क के लिए बेस स्टेशन हैं। वे वायरलेस क्लाइंट के साथ संचार करने के लिए रेडियो फ्रीक्वेंसी प्रसारित करते हैं और प्राप्त करते हैं।

वायरलेस ग्राहक – ये कम्प्यूटिंग डिवाइस हैं जो एक वायरलेस नेटवर्क इंटरफेस कार्ड (WNIC) से लैस हैं। लैपटॉप, आईपी फोन, पीडीए वायरलेस ग्राहकों के विशिष्ट उदाहरण हैं।

कई संगठनों ने वायरलेस LAN को लागू किया है। ये नेटवर्क अभूतपूर्व रूप से बढ़ रहे हैं। इस प्रकार, वायरलेस LAN में खतरों को समझना और नेटवर्क सुरक्षा सुनिश्चित करने के लिए सामान्य निवारक उपाय सीखना महत्वपूर्ण है।

एक वायरलेस LAN (WLAN) एक वायरलेस कम्प्यूटर नेटवर्क है जो एक घर, स्कूल, कम्प्यूटर प्रयोगशाला, परिसर, कार्यालय भवन आदि जैसे सीमित क्षेत्र के भीतर स्थानीय क्षेत्र नेटवर्क (LAN) बनाने के लिए वायरलेस संचार का उपयोग करके दो या अधिक उपकरणों को जोड़ता है। उपयोगकर्ताओं को क्षेत्र के भीतर घूमने की क्षमता देता है और फिर भी नेटवर्क से जुड़ा रहता है। एक प्रवेश द्वार के माध्यम से, एक WLAN भी व्यापक इंटरनेट के लिए एक कनेक्शन प्रदान कर सकता है।

अधिकांश आधुनिक WLAN IEEE 802.11 मानकों पर आधारित हैं और वाई–फाई ब्रांड नाम के तहत विपणन किए जाते हैं। वायरलेस LAN अपनी स्थापना और उपयोग में आसानी के कारण, घर में उपयोग के लिए लोकप्रिय हो गए हैं। वे वाणिज्यिक संपत्तियों में भी लोकप्रिय हैं जो अपने कर्मचारियों और ग्राहकों को वायरलेस एक्सेस प्रदान करते हैं।

वायरलेस LAN के घटकः

पारंपरिक वायर्ड LAN द्वारा आवश्यक घटकों के अलावा, एक वायरलेस LAN को अतिरिक्त घटकों की आवश्यकता होती है। वे रेडियो फ्रीक्वेंसी (RF) या इन्फ्रारेड (IR) पर ट्रांसमीटर और रिसीवर हैं। RF ट्रांसमीटर और रिसीवर को दो–तरफा संचार करने के लिए एंटेना की आवश्यकता होती है। इस क्षेत्र में एंटीना और प्रसार के बारे में व्यापक ज्ञान की आवश्यकता होती है। आमतौर पर एक परीक्षण स्थापना वास्तविक कार्यान्वयन से पहले की जाती है। हब, पुल, नेटवर्क ऑपरेटिंग सिस्टम, सर्वर और अन्य घटक ठीक वैसे ही काम कर रहे हैं जैसे वे एक वायर्ड लैन पर थे।

वायरलेस LAN के कार्यः

वायरलेस LAN किसी भी भौतिक संबंध पर भरोसा किए बिना एक बिंदु से दूसरे बिंदु तक जानकारी संचार करने के लिए विद्युत चुम्बकीय तरंगों (रेडियो या अवरक्त तकनीक) का उपयोग करते हैं। रेडियो तरंगों को अक्सर रेडियो वाहक के रूप में संदर्भित किया जाता है क्योंकि वे बस दूरस्थ रिसीवर तक ऊर्जा पहुंचाने का कार्य करते हैं।

प्रेषित किए जा रहे डेटा को रेडियो वाहक पर सुपरइम्पोज किया जाता है ताकि इसे प्राप्त अंत में सटीक रूप से निकाला जा सके। यह आम तौर पर प्रेषित सूचना द्वारा वाहक के मॉड्यूलेशन के रूप में संदर्भित किया जाता है। रेडियो वाहक पर एक बार डेटा सुपरइम्पोज्ड (मॉड्यूलेटेड) होने के बाद, रेडियो सिग्नल एकल आवृत्ति से अधिक होता है, क्योंकि मोड्यूलिंग सूचना की आवृत्ति या बिट दर वाहक में जुड़ जाती है।

यदि रेडियो तरंगें अलग–अलग रेडियो फ्रीक्वेंसी पर प्रसारित होती हैं, तो एक ही समय में एक ही स्थान पर कई रेडियो वाहक एक ही स्थान पर मौजूद हो सकते हैं। डेटा निकालने के लिए, एक रेडियो रिसीवर एक रेडियो आवृत्ति में धुन करता है जबकि अन्य सभी आवृत्तियों को खारिज कर देता है। एक मूल वायरलेस LAN कॉन्फिगरेशन में, एक ट्रांसमीटर/रिसीवर (ट्रांसीवर) डिवाइस, जिसे एक्सेस पॉइंट कहा जाता है, एक मानक स्थान से वायर्ड नेटवर्क से कनेक्ट होता है, मानक केबलिंग का उपयोग करके। एक्सेस प्वाइंट वायरलेस लैन और वायर्ड नेटवर्क इंफ्रास्ट्रक्चर के मध्य डेटा प्राप्त करता है, बफर्स करता है और डेटा को फिर से ट्रांसमिट करता है।

एक एकल पहुँच बिंदु उपयोगकर्ताओं के एक छोटे समूह का समर्थन कर सकता है और एक सौ से कई सौ फीट से कम की सीमा में कार्य कर सकता है। पहुँच बिंदु (या एक्सेस बिंदु से जुड़ा एंटीना) आमतौर पर उच्च होता है, लेकिन आवश्यक रूप से कहीं भी माउंट किया जा सकता है जो व्यावहारिक है जब तक वांछित रेडियो कवरेज प्राप्त होता है।

अंतिम उपयोगकर्ता वायरलेस लैन एडेप्टर के माध्यम से वायरलेस LAN का उपयोग करते हैं, जो नोटबुक या पामटॉप कम्प्यूटर्स में एड–ऑन कार्ड के रूप में कार्यान्वित किए जाते हैं, डेस्कटॉप कम्प्यूटर में कार्ड के रूप में, या हाथ से पकड़े गए कम्प्यूटर के भीतर एकीकृत होते हैं। वायरलेस LAN एडेप्टर क्लाइंट नेटवर्क ऑपरेटिंग सिस्टम (NOS) और एयरवेब के मध्य एक एंटीना के माध्यम से एक इंटरफेस प्रदान करते हैं। वायरलेस कनेक्शन की प्रकृति NOS के लिए पारदर्शी है।

अनुप्रयोगः

वायरलेस LAN में के कई अनुप्रयोग हैं। WLAN के आधुनिक कार्यान्वयन छोटे इन–होम नेटवर्क से लेकर बड़े, कैंपस–आकार वाले हैं जो हवाई जहाज और ट्रेन पर पूरी तरह से मोबाइल नेटवर्क हैं।

उपयोगकर्ता WLAN के हॉटस्पॉट से रेस्तरां, होटल, और अब पोर्टेबल उपकरणों के साथ इंटरनेट का उपयोग कर सकते हैं जो 3G या 4G नेटवर्क से जुड़ते हैं। अक्सर इस प्रकार के सार्वजनिक पहुँच बिंदुओं को नेटवर्क में शामिल होने के लिए किसी पंजीकरण या पासवर्ड की आवश्यकता नहीं होती है। एक बार पंजीकरण होने और/या शुल्क का भुगतान करने के बाद दूसरों तक पहुँचा जा सकता है।

उपलब्ध वायरलेस LAN इन्फ्रास्ट्रक्चर को उपलब्ध हार्डवेयर में कोई संशोधन के साथ इनडोर पोजिशनिंग सिस्टम के रूप में काम करने के लिए भी उपयोग किया जा सकता है।

WLAN के लाभः

एक WLAN का सबसे स्पष्ट लाभ यह है कि डिवाइस वायरलेस तरीके से कनेक्ट हो सकते हैं, केबल की आवश्यकता को समाप्त कर सकते हैं। यह घरों और व्यवसायों को ईथरनेट के साथ भवन के तारों के बिना स्थानीय नेटवर्क बनाने की अनुमति देता है। यह नेटवर्क से कनेक्ट करने के लिए स्मार्टफोन और टैबलेट जैसे छोटे उपकरणों के लिए एक रास्ता भी प्रदान करता है। WLAN राउटर पर भौतिक पोर्ट की संख्या तक सीमित नहीं हैं और इसलिए दर्जनों या सैकड़ों उपकरणों का समर्थन कर सकते हैं। एक WLAN की सीमा को आसानी से एक या अधिक रिपीटर्स जोड़कर बढ़ाया जा सकता है। अंत में, एक WLAN को नए संस्करणों के साथ राउटर की जगह आसानी से अपग्रेड किया जा सकता है – पुराने ईथरनेट केबल को अपग्रेड करने की तुलना में बहुत आसान और सस्ता समाधान।

WLAN का नुकसानः

वायरलेस नेटवर्क वायर्ड नेटवर्क की तुलना में स्वाभाविक रूप से कम सुरक्षित हैं। कोई भी वायरलेस डिवाइस एक WLAN से कनेक्ट करने का प्रयास कर सकता है, इसलिए सुरक्षा की चिंता होने पर नेटवर्क तक पहुँच को सीमित करना महत्वपूर्ण है। यह आमतौर पर वायरलेस प्रमाणीकरण जैसे WEP या WPA का उपयोग करके किया जाता है, जो संचार को एन्क्रिप्ट करता है। इसके अतिरिक्त, वायरलेस नेटवर्क अन्य संकेतों या भौतिक बाधाओं, जैसे कंक्रीट की दीवारों से हस्तक्षेप करने के लिए अतिसंवेदनशील होते हैं। चूंकि LANs उच्चतम प्रदर्शन और सुरक्षा प्रदान करते हैं, वे अभी भी कई कॉर्पोरेट और सरकारी नेटवर्क के लिए उपयोग किए जाते हैं।

वायरलेस LAN पर हमलेः

वायरलेस LAN पर किए जाने वाले विशिष्ट हमले निम्न हैं –

Eavesdropping: हमलावर डेटा के लिए वायरलेस नेटवर्क की निगरानी करता है, जिसमें प्रमाणीकरण क्रेडेंशियल शामिल हैं।

Masquerading: हमलावर एक अधिकृत उपयोगकर्ता को लागू करता है और वायरलेस नेटवर्क पर पहुँच और विशेषाधिकार प्राप्त करता है।

ट्रैफिक विश्लेषणः हमलावर संचार पैटर्न और प्रतिभागियों की पहचान करने के लिए वायरलेस नेटवर्क के माध्यम से प्रसारण की निगरानी करता है।

सेवा से इनकारः हमलावर वायरलेस LAN या नेटवर्क उपकरणों के सामान्य उपयोग या प्रबंधन को रोकता है या प्रतिबंधित करता है।

संदेश संशोधन/रिप्ले – हमलावर वायरलेस नेटवर्क के माध्यम से भेजे गए एक वैध संदेश को बदल देता है या हटाता है, इसे जोड़कर, बदलकर या फिर से पुनः व्यवस्थित करता है।

वायरलेस लैन में सुरक्षा उपायः

सुरक्षा उपाय हमलों को हराने और नेटवर्क को जोखिम प्रबंधन करने के लिए साधन प्रदान करते हैं। ये नेटवर्क प्रबंधन, संचालन और तकनीकी उपाय हैं। हम वायरलेस LAN के माध्यम से प्रेषित डेटा की गोपनीयता, उपलब्धता और अखंडता सुनिश्चित करने के लिए अपनाए गए तकनीकी उपायों के बारे में नीचे चर्चा करेंगे।

वायरलेस LAN में, एन्क्रिप्शन और क्लाइंट प्रमाणीकरण के माध्यम से सुरक्षा प्रदान करने के लिए सभी APs को कॉन्फिगर किया जाना चाहिए। सुरक्षा प्रदान करने के लिए वायरलेस लैन में उपयोग की जाने वाली योजनाएँ निम्न प्रकार हैं:

वायर्ड समतुल्य गोपनीयता (WEP):

यह वायरलेस नेटवर्क को सुरक्षित करने के लिए 802.11 मानक में निर्मित एक एन्क्रिप्शन एल्गोरिथ्म है। WEP एन्क्रिप्शन 40–बिट/104–बिट कुंजियों और 24–बिट प्रारंभीकरण वेक्टर के साथ RC4 (रिवेस्ट सिफर 4) स्ट्रीम सिफर का उपयोग करता है। यह अंत बिन्दु प्रमाणीकरण भी प्रदान कर सकता है।

हालांकि, यह WEP एन्क्रिप्शन में कई खामियों के रूप में सबसे कमजोर एन्क्रिप्शन सुरक्षा तंत्र है। WEP प्रमाणीकरण प्रोटोकॉल नहीं रखता है। इसलिए, WEP का उपयोग करने की अत्यधिक अनुशंसा नहीं की जाती है।

802.11i प्रोटोकॉलः

इस प्रोटोकॉल में एन्क्रिप्शन के कई और मजबूत रूप संभव हैं। इसे कमजोर WEP योजना को बदलने के लिए विकसित किया गया है। यह प्रमुख वितरण तंत्र प्रदान करता है। यह प्रति स्टेशन एक कुंजी का समर्थन करता है, और सभी के लिए एक ही कुंजी का उपयोग नहीं करता है। यह एक्सेस पॉइंट से अलग ऑथेंटिकेशन सर्वर का उपयोग करता है।

IEEE802.11i, CBC-MAC प्रोटोकॉल (CCMP) के साथ काउंटर मोड नामक प्रोटोकॉल के उपयोग को अनिवार्य करता है। CCMP प्रेषक के हस्तांतरित और प्रामाणिकता की डेटा की गोपनीयता और अखंडता प्रदान करता है। यह उन्नत एन्क्रिप्शन स्टैंडर्ड (AES) ब्लॉक सिफर पर आधारित है।

IEEE802.11i प्रोटोकॉल में संक्रिया के चार चरण हैं। वे निम्न हैं:

STA और AP संचार एल्गोरिथ्म जैसे आपसी सुरक्षा क्षमताओं का संचार और खोज करते हैं।

STA और AS पारस्परिक रूप से प्रमाणित और एक साथ मास्टर कुंजी उत्पन्न करते हैं। AP, "pass through" के रूप में कार्य करता है।

STA ने युग्मवार मास्टर की की व्युत्पत्ति करता है। AS समान PMK प्राप्त करता है और AP को भेजता है।

STA, AP संदेश एन्क्रिप्शन और डेटा अखंडता के लिए उपयोग की जाने वाली टेम्पोरल की (Temporal Key - TK) प्राप्त करने के लिए PMK का उपयोग करते हैं।

अन्य मानक:

वाई–फाई संरक्षित एक्सेस (WPA): यह प्रोटोकॉल IEEE 802.11i मानक के बहुमत को लागू करता है। यह IEEE 802.11i से पहले मौजूद था और एन्क्रिप्शन के लिए RC4 एल्गोरिथम का उपयोग करता है। इसके संचालन के दो तरीके हैं। एंटरप्राइज मोड में, WPA प्रमाणीकरण सर्वर के साथ संचार करने के लिए प्रमाणीकरण प्रोटोकॉल 802.1x का उपयोग करता है, और इसलिए क्लाइंट स्टेशन के लिए पूर्व–मास्टर कुंजी (PMK) विशिष्ट है। पर्सनल मोड में, यह 802.1x का उपयोग नहीं करता है, PMK को पूर्व–साझा कुंजी द्वारा बदल दिया जाता है, जैसा कि लघु कार्यालय गृह कार्यालय वायरलेस LAN वातावरण के लिए उपयोग किया जाता है।

WPA में एक ध्वनि संदेश अखंडता परीक्षण भी सम्मिलित है, जो चक्रीय अतिरेक परीक्षण (Cyclic Redundancy Check - CRC) की जगह लेता है जो WEP मानक द्वारा उपयोग किया जाता था।

WPA2: WPA2 ने WPA का स्थान ले लिया। WPA2, IEEE 802.11i योजना के सभी अनिवार्य अवयवों को लागू करता है। विशेष रूप से, इसमें CCMP के लिए अनिवार्य समर्थन, मजबूत सुरक्षा के साथ AES– आधारित एन्क्रिप्शन मोड सम्मिलित है। इस प्रकार, जहाँ तक हमलों का संबंध है, WPA2/IEEE802-11i WEP कमजोरियों, मानव–मध्य हमलों, जालसाजी पैकेट जालसाजी और फिर से खेलना हमलों के खिलाफ बचाव के लिए पर्याप्त समाधान प्रदान करता है। हालांकि, DoS हमले को ठीक से संबोधित नहीं किया गया है और ऐसे हमलों को मूल रूप से रोकने के लिए कोई ठोस प्रोटोकॉल नहीं हैं क्योंकि ऐसे हमले आवृत्ति बैंड के साथ हस्तक्षेप करने जैसी भौतिक परत को लक्षित करते हैं।

अभ्यास

1. डाटा लिंक लेयर (आंकड़ा कड़ी परत) में सुरक्षा की अवधारणा को विस्तार से समझाइए।
2. सुरक्षित ईथरनेट लैन से क्या समझते हैं?
3. सुरक्षित स्पानिंग ट्री प्रोटोकॉल (सुरक्षित विस्तरित तरू संदेशाचार) पर संक्षिप्त टिप्पणी लिखिए।
4. सुरक्षित आभासी लैन क्या है? समझाइए।
5. सुरक्षित वायरलेस (बेतार) लैन से क्या समझते हैं?

अध्याय – 13

एक्सेस कन्ट्रोल (अभिगम नियंत्रण) और फायरवॉल

नेटवर्क अभिगम नियंत्रण एक व्यक्तिगत संगठनात्मक नेटवर्क की सुरक्षा बढ़ाने की एक विधि है, जो संगठन की सुरक्षा नीति का अनुपालन करने वाले उपकरणों की समाप्ति के लिए नेटवर्क संसाधनों की उपलब्धता को सीमित करता है। एक विशिष्ट नेटवर्क एक्सेस कंट्रोल स्कीम में दो प्रमुख घटक शामिल हैं जैसे कि प्रतिबंधित एक्सेस और नेटवर्क सीमा सुरक्षा।

नेटवर्क उपकरणों के लिए प्रतिबंधित उपयोग उपयोगकर्ता प्रमाणीकरण और प्राधिकरण नियंत्रण के माध्यम से प्राप्त किया जाता है जो नेटवर्क सिस्टम के लिए विभिन्न उपयोगकर्ताओं की पहचान और प्रमाणीकरण के लिए जिम्मेदार है। प्राधिकरण एक संरक्षित संसाधन के लिए विशिष्ट पहुँच अनुमतियाँ देने या अस्वीकार करने की प्रक्रिया है।

नेटवर्क सीमा सुरक्षा नेटवर्क में और वाह्य तार्किक संयोजन को नियंत्रित करती है। उदाहरण के लिए, नेटवर्क सिस्टम पर अनधिकृत पहुँच को रोकने के लिए कई फायरवॉल तैनात किए जा सकते हैं। साथ ही घुसपैठ का पता लगाने और रोकथाम प्रौद्योगिकियों को इंटरनेट से हमलों से बचाव के लिए तैनात किया जा सकता है।

इस अध्याय में, हम विभिन्न प्रकार के फायरवॉल और घुसपैठ का पता लगाने वाली प्रणालियों के बाद नेटवर्क अभिगम के लिए उपयोगकर्ता पहचान और प्रमाणीकरण के तरीकों की चर्चा करेंगे।

13.1 नेटवर्क उपकरणों तक पहुँच सुरक्षित करना:

नेटवर्क पर उपकरणों तक पहुँच को प्रतिबंधित करना नेटवर्क को सुरक्षित करने के लिए एक बहुत ही आवश्यक कदम है। चूंकि नेटवर्क उपकरणों में संचार के साथ–साथ कम्प्यूटिंग उपकरण भी सम्मिलित हैं, इसलिए इनसे समझौता करने से संभवतः संपूर्ण नेटवर्क और इसके संसाधन नीचे आ सकते हैं।

विरोधाभासी रूप से, कई संगठन अपने सर्वर और अनुप्रयोगों के लिए उत्कृष्ट सुरक्षा सुनिश्चित करते हैं लेकिन अल्पविकसित सुरक्षा के साथ संचार उपकरणों को छोड़ देते हैं।

नेटवर्क डिवाइस सुरक्षा का एक महत्वपूर्ण पहलू एक्सेस कंट्रोल और प्राधिकरण है। इन दो आवश्यकताओं को संबोधित करने और उच्च स्तर तक नेटवर्क सुरक्षा को बढ़ाने के लिए कई प्रोटोकॉल विकसित किए गए हैं।

13.2 उपयोगकर्ता प्रमाणीकरण और प्रमाणन:

विशेष रूप से नेटवर्क इन्फ्रास्ट्रक्चर उपकरणों में नेटवर्क सिस्टम तक पहुँच को नियंत्रित करने के लिए उपयोगकर्ता प्रमाणीकरण आवश्यक है। प्रमाणीकरण के दो पहलू हैंः सामान्य पहुँच प्रमाणीकरण और कार्यात्मक प्राधिकरण।

सामान्य पहुँच प्रमाणीकरण यह नियंत्रित करने की विधि है कि किसी विशेष उपयोगकर्ता के पास उस सिस्टम के लिए किसी भी प्रकार का उपयोग सही है जिससे वह कनेक्ट करने का प्रयास कर रहा है। आमतौर पर, इस तरह की पहुँच उस सिस्टम के साथ खाता रखने वाले उपयोगकर्ता से जुड़ी होती है। प्राधिकरण व्यक्तिगत उपयोगकर्ता अधिकारों से संबंधित है। उदाहरण के लिए, यह तय करता है कि उपयोगकर्ता एक बार प्रमाणित होने के बाद क्या कर सकता है? उपयोगकर्ता डिवाइस को कॉन्फिगर करने या केवल डेटा देखने के लिए अधिकृत हो सकता है।

उपयोगकर्ता प्रमाणीकरण उन कारकों पर निर्भर करता है जिनमें वह कुछ जानता है पासवर्ड, क्रिप्टोग्राफिक टोकन, या बायोमेट्रिक है। पहचान और प्रमाणीकरण के लिए एक से अधिक कारकों का उपयोग मल्टीफॉर्मर प्रमाणीकरण के लिए आधार प्रदान करता है।

13.3 पासवर्ड आधारित प्रमाणीकरण:

न्यूनतम स्तर पर, सभी नेटवर्क उपकरणों में उपयोगकर्ता नाम–पासवर्ड प्रमाणीकरण होना चाहिए। पासवर्ड गैर–तुच्छ (कम से कम 10 कैरेक्टर, मिश्रित वर्णमाला, संख्या और प्रतीक) होना चाहिए।

उपयोगकर्ता द्वारा रिमोट एक्सेस की दशा में, उपयोगकर्ता पर यह सुनिश्चित करने के लिए एक विधि का उपयोग किया जाना चाहिए और नेटवर्क पर पासवर्ड स्पष्ट रूप से पारित नहीं किया जाता है। इसके अतिरिक्त, पासवर्ड को कुछ उचित आवृत्ति के साथ भी बदला जाना चाहिए।

13.4 केन्द्रीकृत प्रमाणीकरण विधि:

व्यक्तिगत डिवाइस आधारित प्रमाणीकरण प्रणाली एक बुनियादी अभिगम नियंत्रण उपाय प्रदान करता है। हालांकि, एक केंद्रीकृत प्रमाणीकरण पद्धति को अधिक प्रभावी और कुशल माना जाता है जब नेटवर्क में बड़ी संख्या में डिवाइस होते हैं, जिसमें बड़ी संख्या में उपयोगकर्ता इन उपकरणों तक पहुँचते हैं।

रिमोट नेटवर्क एक्सेस में आने वाली समस्याओं को हल करने के लिए परंपरागत रूप से, केंद्रीकृत प्रमाणीकरण का उपयोग किया गया था। रिमोट एक्सेस सिस्टम (RAS) में, नेटवर्क उपकरणों पर उपयोगकर्ताओं का प्रशासन व्यावहारिक नहीं है। सभी उपकरणों में सभी उपयोगकर्ता जानकारी रखना और फिर उस जानकारी को अद्यतित रखना एक प्रशासनिक दुःस्वप्न है।

केन्द्रीयकृत प्रमाणीकरण प्रणाली, जैसे कि RADIUS और कर्बरोस, इस समस्या को हल करते हैं। ये केंद्रीकृत तरीके उपयोगकर्ता जानकारी को एक स्थान पर संग्रहीत और प्रबंधित करने की अनुमति देते हैं। इन प्रणालियों को आमतौर पर अन्य उपयोगकर्ता खाता प्रबंधन योजनाओं जैसे कि माइक्रोसॉफ्ट की सक्रिय निर्देशिका या LDAP निर्देशिकाओं के साथ समेकित रूप से एकीकृत किया जा सकता है। अधिकांश RADIUS सर्वर सामान्य RADIUS प्रोटोकॉल में अन्य नेटवर्क उपकरणों के साथ संचार कर सकते हैं और फिर निर्देशिकाओं में संग्रहीत खाता जानकारी को सुरक्षित रूप से एक्सेस कर सकते हैं।

उदाहरण के लिए, माइक्रोसॉफ्ट का इंटरनेट प्रमाणीकरण सर्वर (IAS) RADIUS और सक्रिय निर्देशिका को पुल करता है ताकि उपकरणों के उपयोगकर्ताओं के लिए केंद्रीकृत प्रमाणीकरण प्रदान किया जा सके। यह यह भी सुनिश्चित करता है कि उपयोगकर्ता खाता जानकारी माइक्रोसॉफ्ट डोमेन खातों के साथ एकीकृत है।

13.5 एक्सेस नियंत्रण सूची:

कई नेटवर्क उपकरणों को एक्सेस सूची के साथ कॉन्फिगर किया जा सकता है। ये सूचियाँ होस्टनाम या IP पते को परिभाषित करती हैं जो डिवाइस तक पहुँचने के लिए अधिकृत हैं। यह विशिष्ट है, उदाहरण के लिए, नेटवर्क व्यवस्थापक को छोड़कर IP से नेटवर्क उपकरण तक पहुँच को प्रतिबंधित करना।

यह तब किसी भी प्रकार की पहुँच से रक्षा करेगा जो अनधिकृत हो सकती है। इस प्रकार की एक्सेस सूची एक महत्वपूर्ण अंतिम रक्षा के रूप में काम करती हैं और कुछ उपकरणों पर अलग–अलग एक्सेस प्रोटोकॉल के लिए अलग–अलग नियमों के साथ काफी शक्तिशाली हो सकती हैं।

13.6 कम्प्यूटर वायरस:

कम्प्यूटर वायरस के नाम से हम एक पूरे सॉफ्टवेयर के समूह की पहचान करते हैं। इन सभी सदस्यों में एक समानता है : इन सभी में पुनः उत्पादन की क्षमता होती है।

ये सभी कम्प्यूटर के डिस्क सेक्टर से या होस्ट सॉफ्टवेयर से जुडकर पुनः उत्पन्न कर सकते हैं, तथा हमें इसका पता ही नहीं चलता है। वायरस का प्रभाव छोटी–सी समस्या से लेकर विकराल रूप भी धारण कर सकता है।

कुछ वायरस थोड़ी परेशानी मात्र उत्पन्न करते हैं जैसे कि प्रत्येक 10 मिनट में मॉनीटर पर कोई अवांछनीय संदेश देना या पूरी डिस्क पर खुद को कॉपी कर लेना या किसी विशेष प्रकार की फाइल से जुड़ जाना आदि। दूसरी ओर कुछ वायरसों के अत्यंत गंभीर परिणाम हो सकते हैं जैसे कि हार्डडिस्क फॉरमेट कर देना, जिससे हमारा सम्पूर्ण डेटा गायब हो सकता है। कुछ अन्य वायरस मदर बोर्ड को भी खराब कर सकते हैं। जो परेशानियों के साथ–साथ खर्च भी बढ़ा देता है।

कुछ वायरस तथा ऐसे ही सॉफ्टवेयर हाल ही में काफी सुर्खियों में रहे हैं। इनमें I LOVE YOU, KLEZ, CODE RED, NIMDA, MELIZZA, REDLOF, BLASTER तथा CIH प्रमुख हैं। BLASTER वार्म 30 मिनिट में 330 हजार कम्प्यूटर को संक्रमित करता है। ये कम्प्यूटर मुख्यतः विंडोज ऑपरेटिंग सिस्टम चला रहे होते हैं। BLASTER आम एंटीवायरस से बेअसर रहता है तथा इसमें इंटरनेट पर कार्य को अवरूद्ध करने की क्षमता है। BLASTER के द्वारा वायरस बनाने वाले संक्रमित सिस्टम से डेटा को पढ़ सकते या खराब कर सकते हैं।

बूट सेक्टर वायरसः

यह वायरस हार्ड डिस्क या फ्लॉपी डिस्क के बूट सेक्टर को संक्रमित करता है। जैसे ही कम्प्यूटर "on" किया जाता है यह वायरस मेमोरी में लोड हो जाता है। एक बार शुरू होने के पश्चात यह वायरस डिस्क से डिस्क जाते हुए खुद को कापी कर सकता है। Brain एक प्रकार का बूट वायरस है। फ्लॉपी डिस्क के प्रयोग में गिरावट से इस प्रकार के वायरस आजकल कम प्रचलन में हैं। अतिविकसित बूट सेक्टर वायरस अब Multi-partite वायरस में तब्दील हो गये हैं।

फाईल संक्रमित वायरसः

यह वायरस निष्पादन प्रोग्राम से जुड जाते हैं। यह सामान्यतः अपने कोड को एन्क्रिप्ट कर देते हैं जिससे उनकी उपस्थिति का पता नहीं चलता है। इस प्रकार का वायरस सम्बंधित फाइल को प्रारम्भ करने के निष्पादन कमांड को वश में कर लेते हैं। कमाण्ड देने पर पहले यह खुद चलते है तथा इसके पश्चात यह कमाण्ड की मूल फाइल को चला देते है जिससे सिस्टम सामान्य कार्य करता प्रतीत होता है।

यह वायरस अन्य निष्पादन योग्य फाईल से जुड़ जाता है तथा अपना एक हस्ताक्षर–सा छोड़ जाता है जिससे वह किसी एक ही फाइल को पुनः संक्रमित न करे। यह वायरस विशेष तकनीक के जरिए छुप सकता है तथा इन्हें ढूंढना काफी कठिन कार्य है।

W32/CIH.SPACEFILLER एक प्रकार का फाईल संक्रमित वायरस है। यह एक खतरनाक वायरस है जो हमारे कम्प्यूटर के BIOS पर भी लिख देता है। यह टुकड़ों में बॅटकर फाइल्स के मध्य में छुप जाता है जिससे इसे ढूँढना मुश्किल हो जाता है।

मैक्रो वायरसः

यह वायरस मैक्रो पर प्रहार करता है। एमएस–ऑफिस जैसे उत्पाद में मैक्रो प्रयोग में आते हैं। मैक्रो के द्वारा एमएस–वर्ड तथा एमएस–एक्सेल में कुछ कार्यो कों स्वतः करने की क्षमता आ जाती है। इसमें विजुअल बेसिक भाषा का एक रूप प्रयुक्त होता है। सर्वप्रथम मैक्रो वायरस का नाम कॉन्सेप्ट था। एमएस–वर्ड में मैक्रो की क्षमता समाहित होते ही यह वायरस निकाला गया।

मैक्रो तथा स्क्रिप्ट वायरस आज काफी प्रचलन में हैं। स्क्रिप्ट वायरस तथा मैक्रो वायरस में एक महत्वपूर्ण अन्तर यह है कि स्क्रिप्ट वायरस बहु उत्पाद वातावरण में काम कर सकते है। VB स्क्रिप्ट भाषा का कोड Web Server, Browser, Microsoft outlook इत्यादि में चल सकता है। स्क्रिप्टिंग भाषा के द्वारा वायरस के लेखक संक्रमित कम्प्यूटर पर मैक्रो भाषा के स्थान पर अधिक नियंत्रण देते हैं।

Multi-Partite वायरसः

यह दोहरा किस्म का वायरस है। इसे बूट सेक्टर वायरस तथा फाईल संक्रमित वायरस का मेल कह सकते हैं। यह संकमित फाइलों के द्वारा फैलता है तथा खुद को बूट सेक्टर में लोड कर देता है। यह चक्र चलता जाता है। अधिकतर नये प्रकार के वायरस इसी श्रेणी में आते हैं।

स्क्रिप्ट वायरसः

स्क्रिप्ट वायरस अपने कार्य करने हेतु किसी स्क्रिप्टिंग भाषा पर आश्रित रहते हैं। उन्हें एक होस्ट वातावरण की भी आवश्यकता होती है। जो उनके कमाण्ड को ठीक से समझ सके। संक्रमण करने का एजेन्ट टेक्स्ट फाईल भी हो सकती है, जैसा कि mIRC स्क्रिप्ट वायरस में देखा जाता है।

स्क्रिप्ट वायरस मैक्रो वायरस से अलग होते हैं। यह अन्तर हम पहले ही मैक्रो वायरस के अन्तर्गत देख चुके हैं। VBS/Bubbleboy, VBS/Redlof कुछ प्रचलित स्क्रिप्ट वायरस हैं। VBS/Bubbleboy किसी ई–मेल संदेश से ही रन कर सकता है।

ट्रोजन हॉर्स प्रोग्रामः

बाहरी तौर पर यह सॉफ्टवेयर मान्य से लगते हैं परन्तु भीतरी तौर पर यह ज्यादातर हानिकारक प्रोग्राम ही होते हैं। इन्हें वायरस नहीं कहा जाता है, क्योंकि इनमें पुनः उत्पादन की क्षमता नहीं होती है।

ट्रोजन हॉर्स पूरी तरह से उपयोगकर्त्ता की मानसिकता पर निर्भर करते हैं। इरादा यही होता है कि उपयोगकर्त्ता इन्हें कम से कम एक बार अवश्य चलाये। कुछ ट्रोजन हॉर्स अपने माहौल की नकल भी कर लेते हैं, जिससे उन्हें अपना कार्य करने का मौका मिल जाये।

कई ट्रोजन हॉर्स Compuserve तथा America Online जैसी लोकप्रिय सेवाओं से गोपनीय जानकारी जैसे पासवर्ड आदि चुरा लेते हैं। चुराने वाला व्यक्ति पासवर्ड का गलत फायदा उठा सकता है। यह प्रोग्राम Buddylist.exe या Winserver.exe नाम के अन्तर्गत नजर आ जाते हैं।

वॉर्मः

यह एक ऐसा सॉफ्टवेयर है जिसमें पुनः उत्पादन की क्षमता नहीं है। यह अप्रत्यक्ष रूप से फैलता है। यह ई–मेल के सिस्टम पर कब्जा कर लेता है तथा फिर सैकड़ों उपयोगकर्त्ता को कॉपी भेज देता है। इसके अतिरिक्त यह ज्यादा चलने वाली वेबसाइट पर स्वयं को डाउनलोड हेतु उपलब्ध करा देता है।

वॉर्म की विध्वंसक ताकत तथा फैलने की क्षमता वायरस के ही समान है। यह आमतौर पर उपयोगकर्त्ता को उन्हें डाउनलोड करने के लिए उकसाते हैं।

W97M/MELISSA जो MELISSA वायरस के नाम से जाना जाता है, काफी तेज गति से फैलता है। इसके लिए वह ई–मेल सिस्टम का सहारा लेता है। अति तीव्र फैलाव से यह कई बार संक्रमित करता है तथा इसके चलते कई ई–मेल सर्वर खराब हो जाते हैं।

13.7 एण्टी वायरसः

जैसे–जैसे हम अधिकाधिक वायरस इत्यादि का सामना कर रहें हैं, हमारे कम्प्यूटर की रक्षा की महत्ता और बढ़ जाती है। एंटीवायरस सॉफ्टवेयर हमारे कम्प्यूटर को वायरस के हमले से बचाते हैं। एंटीवायरस सॉफ्टवेयर एक ना थकने वाले सुरक्षाकर्मी की तरह कार्यरत रहता है। जब भी हम कार्य कर रहे होते हैं यह एंटीवायरस पीछे ही पीछे चल रहा होता है।

आमतौर पर संक्रमित फाइल मिलने पर एंटीवायरस निम्नांकित कार्य करता है :–

File Cleaning - इसमें वायरस हटा दिया जाता है जबकि फाइल वहीं रहती है।

File Deleting - इसमें पूरी फाइल ही हटा दी जाती है।

File Quarantining - इसमें संक्रमित फाइल को अन्य फाइल्स से अलग एक कोने में कर दिया जाता है जिससे संक्रमण के फैलने की आशंका कम से कम हो जाती है।

Ignoring the virus - वायरस सक्रंमित फाइल को उसी स्थिति में रखना।

आधुनिक एंटीवायरस ई–मेल के द्वारा आने वाले वायरस को भी पहचान लेते हैं। दिन प्रतिदिन नये प्रकार के वायरस आ रहे हैं। अतः हमें एंटीवायरस सॉफ्टवेयर को कदम–कदम पर अद्यतन करना पड़ता है। अन्यथा वह नये वायरस को पहचान नहीं पायेगा।

नेटवर्क पर वायरसः

कुछ समय पहले कम्प्यूटर उपयोगकर्त्ता वायरस के बारे में इतने चिन्तित नही होते थे। वायरस के सम्पर्क में आने के काफी कम मौके थे। आजकल कई कम्प्यूटर उपयोगकर्त्ता संदेश भेजना, डेटा का एक दूसरे से आदान–प्रदान करना आदि कार्य नेटवर्क, फ्लॉपी डिस्क/हार्ड डिस्क तथा इंटरनेट के द्वारा भी करते हैं। ऐसे में वायरस से बचाव अत्यंत आवश्यक हो गया है। वायरस–रोधी रणनीति महज एक आधुनिकता समेटे शब्द नहीं है।

हमारे कम्प्यूटर का डेटा कई महीनों या सालों की मेहनत तथा काफी पूँजी निवेश के बाद बनता है। यदि कोई वायरस इसका सफाया कर दे तो हमारी सारी मेहनत तथा पूँजी व्यर्थ जायेगी। सम्भव है कि इस डेटा का पुनर्निर्माण बहुत जटिल अथवा असम्भव भी हो। इसके अलावा नेटवर्क पर अन्य कम्प्यूटर भी वायरस की चपेट में आ सकते हैं।

कुछ समय पहले कम्पनियॉ डेस्कटॉप एन्टीवायरस के द्वारा बचाव करती थीं। Trend Micro जैसी एन्टीवायरस कम्पनियॉ एक दूसरी रणनीति का समर्थन करती हैं। इनके अनुसार वायरस को कॉरपोरेट गेटवे पर रोकना ही सबसे बड़ी समझदारी है। शोध–आधारित कम्पनी IDC के अनुसार गेटवे फिल्टरिंग आज एंटीवायरस के बाजार का सबसे तेजी से बढ़ता हिस्सा है। अतः इस बाजार में आने वाले 2 वर्षों में 34 प्रतिशत वृद्धि की सम्भावना है। फिलहाल Trend Micro इस बाजार में अग्रणी है तथा इसका 45 प्रतिशत बाजार पर कब्जा है।

गेटवे पर फिल्टर करने हेतु मूल सिद्धांत यह है कि SMTP, HTTP तथा FTP पर नियंत्रण रखा जाये। गेटवे ही इस खतरे को सबसे पहले भॉपता है। अन्तिम उद्देश्य यह है कि नेटवर्क पर वायरस का खतरा न्यूनतम कर दिया जाये। नेटवर्क के अन्दर वायरस के प्रवेश में SMTP की सबसे बड़ी गलती होती है। अनुमान है कि 87 प्रतिशत वायरस SMTP के द्वारा ही अन्दर प्रवेश करते हैं।

IDC के अनुसार गेटवे पर एंटीवायरस सुरक्षा किसी भी बड़ी कम्पनी के लिए अत्यंत महत्वपूर्ण है। हालॉकि गेटवे फिल्टरिंग ही सब कुछ नहीं है। कम्पनियों को अपना पूरा नेटवर्क बचाना चाहिये ना कि कोई एक विशेष पॉइन्ट। विशेषज्ञों के अनुसार इस मद के लिये 10 से 20 प्रतिशत का प्रावधान सर्वथा उचित होगा। हाल ही के अत्यंत विध्वंसक क्षमता वाले वायरसों के चलते एक अच्छे फायरवॉल सिस्टम की अत्यधिक आवश्यकता है। फायरवॉल एक ''आग की दीवार'' सा कार्य करते है। फायरवॉल एक विशेष प्रकार का सॉफ्टवेयर है। इसके द्वारा हम यह तय कर सकते हैं कि कौन सा डेटा या प्रोग्राम नेटवर्क में प्रवेश करेगा तथा किसे बाहर ही रोक दिया जायेगा। इस तरह से नेटवर्क में कार्यरत पी.सी. वायरस तथा वार्म के प्रहार से सुरक्षित रहेंगे।

वायरस से बचावः सावधानियाँः

यहाँ पर कुछ ऐसी सावधानियाँ बताई जा रही हैं जिनके पालन करने से वायरस के प्रकोप से काफी हद तक बचा जा सकता है :–

1. कभी भी किसी अनजानी फ्लॉपी डिस्क का प्रयोग तब तक न करें जब तक यह सुनिश्चित न हो जाए कि वह डिस्क संक्रमण से मुक्त है।

2. सभी मूल EXE तथा COM फाइल्स की प्रति एक राइट प्रोटेक्ट (Write Protect) डिस्क में सुरक्षित रखें।

3. जहाँ तक संभव हो कम्प्यूटर खेल न खेलें या इन खेलों के लिए एक अलग बूट डिस्क का निर्माण करके रखें और खेलने के पश्चात किसी अन्य सॉफ्टवेयर का प्रयोग करने से पूर्व कम्प्यूटर का स्विच ऑफ करना न भूलें। ऐसी स्थिति में यदि वायरस मेमोरी में होगा तब भी कम्प्यूटर कें बंद होते ही नष्ट हो जाएगा। तथा अन्य सॉफ्टवेयर का संक्रमण से बचाव हो सकेगा।

4. यदि कभी वायरस का प्रवेश किसी डिस्क में हो जाए तो संक्रमित डिस्क को निर्धारित वायरस के टीके का उपयोग करके वायरस रहित कर ले तथा फिर उसका उपयोग करें ताकि संक्रमण और अधिक न फैले।

5. प्रत्येक डिस्क को जहां तक संभव हो राइट प्रोटेक्ट करके रखें।

6. वायरस के प्रभाव को रोकने के लिए समय–समय पर डिस्क का विश्लेषण ''पी.सी. टूल्स'', ''नॉरटन प्रोग्राम'' या ''वायरस खोजी प्रोग्राम'' की सहायता से करते रहें।

7. हमेशा इस बात का ध्यान रखें कि अपने कम्प्यूटर को किसी अनजानी डिस्क से CTRL-ALT-DEL से बूट न करें।

8. किसी भी सॉफ्टवेयर की जॉली या अवैध प्रति का उपयोग न करें। हमेशा सही प्रति ही खरीदें।

उपर्युक्त सावधानियों का पूर्णतः पालन करने पर काफी हद तक इन वायरसों के संक्रमण से बचा जा सकता है, इतने पर भी यदि किसी वायरस का आक्रमणा आपके कम्प्यूटर पर हो जाए तब आप सूचना प्राप्त होते ही कम्प्यूटर को बंद कर दें तथा किसी कम्प्यूटर विशेषज्ञ को बुलाकर उन वायरसों को अपने कम्प्यूटर में से नष्ट कर दीजिये।

13.8 फायरवॉल:

फायरवॉल कम्प्यूटर सिस्टम या नेटवर्क का एक हिस्सा है जिसका निर्माण अनाधिकृत उपयोग को रोकने और अधिकृत संप्रेषण को अनुमति देने के लिए किया जाता है। यह एक उपकरण या उपकरण का सेट है जो उस तरह कॉन्फिगर किया गया है जो अन्य सुरक्षा डोमेन के बीच कम्प्यूटर यातायात को अनुज्ञा, अस्वीकार, एन्क्रिप्ट, डिक्रिप्ट या प्रोक्सी (अन्दर और बाहर) करता है जिसका आधार कई नियम और अन्य मानक है। फायरवॉल को हार्डवेयर या सॉफ्टवेयर, या दोनों के संयोजन में कार्यान्वित किया जा सकता है। फायरवॉल का प्रयोग अनाधिकृत इन्टरनेट उपयोगकर्ताओं को इन्टरनेट से जुड़े व्यक्तिगत नेटवर्क, मुख्यतः इंट्रानेट का प्रयोग करने से रोकने के लिए किया जाता है। सभी संदेश जो इंट्रानेट से बाहर जाते है या अन्दर प्रवेश करते है वह फायरवॉल के माध्यम से जाते है। फायरवॉल सभी संदेशो की जाँच करता है और जो सन्देश निर्देशित सुरक्षा मानदंडों को पूरा नहीं करते उनको रोकता है।

फायरवॉल तकनीकों के कई प्रकार हैं:

1. पैकेट फिल्टरः पैकेट फिल्टर नेटवर्क के माध्यम से गुजरने वाले हर पैकेट का निरीक्षण करता है और उपयोगकर्ता के परिभाषित नियमों के आधार पर पैकेट को स्वीकार या खारिज करता है। हालांकि यह कॉन्फिगर करने में मुश्किल है, पर काफी प्रभावी है और ज्यादातर अपने उपयोगकर्ताओं के लिए पारदर्शी है। इसमें आईपी स्पूफिंग की संभावना है।
2. एप्लीकेशन गेटवेः एफटीपी और टेलनेट सर्वर जैसे विशिष्ट अनुप्रयोगों के लिए सुरक्षा व्यवस्था लागू करता है। यह बहुत प्रभावी है लेकिन इसके कार्य में गिरावट आ सकती हैं।
3. सर्किट लेवल गेटवेः जब TCP या UDP संबंध स्थापित होता है तब सुरक्षा प्रणाली लागू करता है। एक बार संपर्क हो जाने के बाद, आगे की जाँच के बिना पैकेट होस्ट के बीच प्रवाह कर सकते हैं।
4. प्रॉक्सी सर्वरः नेटवर्क से अन्दर प्रवेश करते या बाहर जाते सभी संदेश को अवरोध करता है। प्रॉक्सी सर्वर प्रभावी ढंग से नेटवर्क के सही पते को छुपाता है।

कार्यविधिः

फायरवॉल एक समर्पित उपकरण, या एक कंप्यूटर है, जो इससे गुजरने वाले नेटवर्क यातायात का निरीक्षण करता है और नियमों के आधार पर मार्ग अस्वीकृत या पारित होने देता हैं।

यह एक सॉफ्टवेयर या हार्डवेयर है जो आम तौर पर एक सुरक्षित नेटवर्क और एक असुरक्षित नेटवर्क के बीच में रखा जाता है और यह एक द्वार की तरह कार्य करता है जो सुनिश्चित करता है की कोई भी निजी चीज बाहर नहीं जा रही है और दुर्भावनापूर्ण चीज अंदर नहीं आ रही है।

फायरवॉल का मूल कार्य अलग विश्वास स्तर के कंप्यूटर नेटवर्क के बीच यातायात प्रवाह के स्तर का नियमन करता है। विशिष्ट उदाहरण है इंटरनेट जो एक क्षेत्र है जिसके ऊपर भरोसा नहीं है और आंतरिक नेटवर्क जो उच्च विश्वास का एक क्षेत्र है। मध्यवर्ती विश्वास स्तर का एक क्षेत्र, जो इंटरनेट और एक भरोसेमंद आंतरिक नेटवर्क के बीच स्थित है, उसे अक्सर परिधि नेटवर्क या असैनिकीकरण किया हुआ क्षेत्र के रूप में जाना जाता है।

फायरवॉल का नेटवर्क में कार्य, एक भवन निर्माण के भीतर आग दरवाजे की दीवार के समान है। पूर्व के मामले में, यह निजी नेटवर्क में घुसपैठ को रोकने का कार्य करता है बाद के मामले में, संरचनात्मक आग को पास की संरचनाओं में फैलने से रोकने और देर करने का कार्य करता है।

इतिहासः

- शब्द फायरवॉल/फायरब्लॉक का मतलब मूल रूप से एक दीवार है जो इमारत के भीतर की आग या संभावित आग को प्रतिबंधित करने के लिए होती है, cf फायरवॉल (निर्माण)। बाद के उपयोग में समान संरचना के सन्दर्भ में, जैसे धातु पत्र जो इंजन डिब्बे में और हवाई जहाज में यात्री डिब्बे अलग करने में आता है।
- जब वैश्विक उपयोग और संपर्क के मामले में इंटरनेट काफी नई तकनीक था तब 1980 में फायरवॉल तकनीक उभरी। नेटवर्क सुरक्षा के लिए फायरवॉल से पहले राउटर्स थे जो नेटवर्क को एक दूसरे से अलग करने के लिए 1980 के दशक के अंत में इस्तेमाल किये गए थे।

- अपेक्षाकृत इन्टरनेट उपयोगकर्ताओं के छोटे समुदाय के विचार, जो बंटवारे और सहयोग करने के लिए खुले थे, को इंटरनेट सुरक्षा के काफी भंग होने जो 1980 के अंत में हुआ, की वजह से समाप्त हो गए।
- क्लिफर्ड स्टोल की जर्मन जासूस की अपने सिस्टम के साथ छेड़छाड़ की खोज।
- बिल चेषविक की शाम बर्फ्रेड के साथ 1992 में जिसमे उन्होंने एक सरल इलेक्ट्रॉनिक जेल बनाया जिसमे हमलावर पर नजर रख सके।
- 1988 में नासा एम्स अनुसंधान केन्द्र कैलिफोर्निया से एक कर्मचारी ने अपने सहयोगियों को एक ईमेल भेजा, जो था।

  We are currently under attack from an Internet VIRUS! It has hit Berkeley, UC San Diego, Lawrence Livermore, Stanford, and NASA Ames.
- मॉरिस वॉर्म खुद को समय की मशीनों में एकाधिक कमजोरियों के माध्यम से फैलता है। हालांकि वो दुर्भावनापूर्ण इरादे में नहीं था, मॉरिस वॉर्म इंटरनेट सुरक्षा पर पहला बड़े पैमाने का हमला था, ऑनलाइन समुदाय ना ही एक हमले की उम्मीद में था और ना ही उससे निपटने के लिए तैयार था।

प्रथम पीढीः

फायरवॉल प्रौद्योगिकी पर पहला समाचार पत्र 1988 में प्रकाशित हुआ, जब डिजिटल उपकरण निगम के इंजीनियर ने पैकेट फिल्टर रूप में परिचित फिल्टर प्रणाली बनाया। एक उच्च विकसित और तकनीकी इंटरनेट सुरक्षा सुविधा के मामले में यह पहली पीढ़ी की काफी बुनियादी प्रणाली थी। एटी एंड टी बेल लेबोरेटरीज, के बिल चेषविक और स्टीव बेलोविन पैकेट फिल्टर पर अपना संशोधन कर रहे थे और अपनी कंपनी के लिए मूल पहली पीढ़ी के वास्तुशिल्प पर आधारित मॉडल विकसित कर रहे थे।

पैकेट जो इंटरनेट पर डेटा को ट्रान्सफर करने के लिए बुनियादी इकाई है उसका निरीक्षण करने का काम पैकेट फिल्टर करते है। यदि पैकेट, पैकेट फिल्टर के नियमों के सेट को मैच करता है तो पैकेट फिल्टर पैकेट को छोड़ (चुपचाप निकाल) देता है या अस्वीकार (त्याग करता है और स्रोत को त्रुटि की प्रतिक्रियाएं भेजता है) करता है।

इस प्रकार का पैकेट फिल्टर, पैकेट यातायात के एक मौजूदा धारा का हिस्सा है की नहीं है उस पर कोई ध्यान नहीं देता (यह कनेक्शन स्टेट पर कोई जानकारी का भंडार नहीं करता)। इसके बजाय, यह पैकेट में हीनिहित जानकारी के आधार पर हर एक पैकेट को फिल्टर करता है (सबसे अधिक पैकेट के स्रोत, गंतव्य पता और प्रोटोकॉल का संयोजन करके और TCP और UDP के लिए बंदरगाह संख्या का उपयोग करते है)।

सबसे ज्यादा संचार TCP और UDP प्रोटोकॉल से होता है और क्योंकि TCP और UDP प्रख्यात पोर्ट का उपयोग यातायात सम्मेलन में अच्छी तरह से प्रयोग करते हैं, इसलिए यातायात का विशेष प्रकार, राज्यविहीन पैकेट फिल्टर के बीच के अंतर को अलग कर सकता हैं और इस तरह के यातायात का नियंत्रण कर सकता है, जाना जाता है, यातायात के उन प्रकार के ऐसे (के रूप में वेब ब्राउजिंग, दूरदराज के मुद्रण, ईमेल प्रेषण, फाइल स्थानांतरण), जब तक कि पैकेट फिल्टर के प्रत्येक पक्ष पर मशीनों दोनों ही गैर मानक पोर्ट का उपयोग कर रहे हैं।

पैकेट फिल्टर फायरवॉल OSI संदर्भ मॉडल के पहले तीन परतों पर काम करता है जिसका मतलब है कि सभी नेटवर्क और शारीरिक परतों के बीच काम होता है। जब एक पैकेट स्रोत से निकलता है और फायरवॉल के माध्यम से जाता है तब उपकरण फायरवॉल में कॉन्फिगर हुए पैकेट फिल्टर के किसी भी नियम से मैच करता है और तदनुसार पैकेट को ड्रॉप या खारिज करता है। जब पैकेट फायरवॉल से होकर गुजरता है तब वो प्रोटोकॉलपोर्ट संख्या के आधार पर पैकेट फिल्टर करता है।

द्वितीय पीढीः

अनुप्रयोग परत को छानने के मुख्य लाभ यह है कि यह कुछ अनुप्रयोगों और प्रोटोकॉल को समझ सकता हैं (जैसे कि फाइल ट्रांसफर प्रोटोकॉल, डीएनएस, या वेब ब्राउजिंग), और यह पता लगा सकते हैं कि अवांछित प्रोटोकॉल गैर मानक पोर्ट के माध्यम से घुसा जा रहा है या फिर प्रोटोकॉल का किसी भी तरह से हानिकारक दुरुपयोग किया जा रहा है। पैकेट फिल्टर फायरवॉल की तुलना में आवेदन फायरवॉल अधिक सुरक्षित और विश्वसनीय है क्योंकि वह OSI संदर्भ मॉडल के सभी सात परत पर काम करता है मतलब आवेदन पत्र से भौतिक परत तक।

यह एक पैकेट फिल्टर फायरवॉल के समान है, लेकिन यहाँ हम सामग्री के आधार पर जानकारी फिल्टर भी कर सकते हैं। आवेदन फायरवॉल का सबसे अच्छा उदाहरण ISA (इंटरनेट सुरक्षा और गति है) सर्वर है। एक आवेदन फायरवॉल उच्च परत प्रोटोकॉल फिल्टर कर सकते हैं जैसे FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP और TFTP (GSS)। उदाहरण के लिए, यदि कोई संगठन को 'विव' शब्द से संबंधित सभी जानकारी को ब्लॉक करना है तो विशेष रूप से शब्द खंड के लिए फायरवॉल पर फिल्टर सामग्री सक्रिय किया जा सकता है। यह एक सॉफ्टवेयर आधारित फायरवॉल है और इस तरह यह स्टेटफुल फायरवॉल की तुलना में बहुत धीमी है।

तृतीय पीढीः

एटी एंड टी बेल लेबोरेटरीज, के तीन सहयोगियों डेव प्रेसेतो, जनार्दन शर्मा और क्षितिज निगम ने 1989—1990 में तीसरी पीढ़ी के फायरवॉल का विकास किया, उन्हें सर्किट स्तर फायरवॉल कहा जाता है।

स्थान के संबंध में प्रत्येक पैकेट को पैकेट श्रृंखला के भीतर रखने का काम भी तीसरी पीढ़ी के फायरवॉल का था। यह प्रौद्योगिकी आम तौर पर एक स्टेटफुल पैकेट निरीक्षण के रूप में जाना जाता है क्योंकि यह फायरवॉल से गुजर रहे सब कनेक्शन का रिकॉर्ड रखता है और निश्चित रूप से पता लगाने के काबिल है कि क्या पैकेट या तो एक नए कनेक्शन की शुरुआत का है, मौजूदा कनेक्शन का एक हिस्सा है, या अवैध पैकेट है। हालांकि अभी भी ऐसे फायरवॉल में स्थिर नियमों का एक सेट है, कनेक्शन की दशा ही एक मापदंड है जो विशिष्ट नियमों को ट्रिगर करते है। इस प्रकार के फायरवॉल मौजूदा कनेक्शन के शोषण और कुछ डेनियल सेवा के हमलों को रोकने में मदद कर सकता हैं।

1992 में, बॉब ब्रादें और इनत देस्चों दक्षिणी कैलिफोर्निया विश्वविद्यालय (युएससी) में एक फायरवॉल की संकल्पना को परिष्कृत कर रहे थे। वीसास के नाम से जानी जाने वाली पहली उपकरण प्रणाली थी जिसमे रंगों और आइकोन के साथ दृश्य एकीकरण अंतरफलक था जो माइक्रोसोफ्ट ज्ञात उत्पाद विंडोज या एप्पल मेक ओएस।

कम्प्यूटर ऑपरेटिंग सिस्टम पे आसानी से उपलब्ध और निर्माण किया जा सकता है। 1994 में इजरायल की एक कंपनी चेक प्वाइंट सॉफ्टवेयर प्रौद्योगिकी ने आसानी से उपलब्ध फायरवॉल—1 सॉफ्टवेयर के रूप में उस पर बनाया।

आधुनिक फायरवॉल की मौजूदा गहरी पैकेट निरीक्षण कार्यशीलता को घुसपैठनिवारण प्रणाली(आईपिएस) द्वारा फैलाया जा सकता है।

वर्तमान में, इंटरनेट इंजीनियरी टास्क फोर्स (आईईटीएफ) का मिडलबॉक्स संचार कार्य का समूह प्रबंधन, फायरवॉल और अन्य मिडलबॉक्स के लिए प्रोटोकॉल के मानकीकरण पर काम कर रहा है।

विकास की एक और अक्ष, फायरवॉल नियमों में उपयोगकर्ताओं की पहचान का एकीकरण के बारे में है। उपयोगकर्ता पहचान IP और ed पते से बांधकर कई फायरवॉल इस तरह की सुविधाओं उपलब्ध करते है जो बहुत अनुमानित है और उसे आसानी से चारों ओर बदला सकता है। NuFW फायरवॉल प्रत्येक कनेक्शन के लिए उपयोगकर्ता के हस्ताक्षर के अनुरोध द्वारा वास्तविक पहचान आधारित फायरवॉल प्रदान करता है। फायरवॉल के कई वर्गीकरण है जो संचार होने की जगह, संचार रुकने की जगह और दशा के अनुरेखण के उपर निर्भर है।

नेटवर्क परत और पैकेट फिल्टर

नेटवर्क परत फायरवॉल जो पैकेट फिल्टर भी कहे जाते है वो टीसीपी आईपी प्रोटोकॉल के अपेक्षाकृत कम स्तर पर संचालित होते है। जब तक वे शासन की स्थापना के नियमों से मेल नहीं खाते तब तक पैकेट को फायरवॉल के माध्यम से गुजारने की अनुमति नहीं मिलती। फायरवॉल प्रशासक नियमों को परिभाषित कर सकते हैं या डिफॉल्ट नियम लागू कर सकते हैं। शब्द पैकेट फिल्टर बीएसडी ऑपरेटिंग सिस्टम के संदर्भ में जन्मा हुआ है। नेटवर्क परत फायरवॉल आम तौर पर दो उप श्रेणियों स्टेटफुल और स्टेटलेस में गिने जाते हैं। स्टेटफुल फायरवॉल सक्रिय सत्र के बारे में संदर्भ को बनाए रखते है और पैकेट प्रसंस्करण गति के लिए वो राज्य सूचना का उपयोग करते है।

किसी भी मौजूदा नेटवर्क कनेक्शन को कई गुण द्वारा वर्णित किया जा सकता है जैसे की स्रोत और गंतव्य आईपी पता, TCP या UDP पोर्ट और कनेक्शन के जीवन का वर्तमान चरण (सत्र दीक्षा, हेन्डशेकिंग, आंकड़ा अंतरण, या पूरा कनेक्शन) यदि एक पैकेट एक मौजूदा कनेक्शन से मेल नहीं खाता, तो उसका एक नए कनेक्शन के लिए नियमो के अनुसार मूल्यांकन किया जाता हैद्य फायरवॉल के दशा फलक के साथ तुलना के आधार पर यदि पैकेट कनेक्शन से मैच करता है तो बिना कोई प्रसंस्करण के उसे पारित किया जाता है।

दशाविहीन फायरवॉल को कम स्मृति की आवश्यकता होती है और सरल फिल्टर के लिए तेज हो सकता है जो फिल्टर करने के लिए लुकअप सत्र से कम समय लेते है। वे दशाविहीन नेटवर्क प्रोटोकॉल जिसमे सत्र की धारणा नहीं होती उसमे भी फिल्टर करने के लिए आवश्यक हो सकती है। हालांकि, वे मेजबानों के बीच का संचार किस स्तर तक पहुँच चुका हैं उसके आधार पर अधिक जटिल निर्णय नहीं कर सकता।

आधुनिक फायरवॉल कई पैकेट विशेषताओं पर आधारित आईपी पता फिल्टर यातायात सकते हैं, स्रोत पोर्ट, गंतव्य आईपी पता या पोर्ट, गंतव्य सेवा जैसे डब्ल्यूडब्ल्यूडब्ल्यू या एफटीपी का फिल्टर कर सकते है। वे प्रोटोकॉल, टीटीएल मूल्यों, लेखक के स्रोत के नेटब्लोक, और कई अन्य गुण के आधार पर फिल्टर कर सकते हैं।

यूनिक्स के विभिन्न संस्करणों पर सामान्य इस्तेमाल होने वाले पैकेट फिल्टर आइपिएफ (विभिन्न), आइपिएफडब्ल्यू (फ्रीबीएसडी) ओएस एक्स, पीएफ (ओपनबीएसडी और अन्य सभी बीएसडी), आईपीटेबल्स पीएफ (ओपनबीएसडी और अन्य सभी बीएसडी), आईपीटेबल्स ।

आवेदन–परत

अनुप्रयोग परत–फायरवॉल टीसीपी आईपी के आवेदन स्तर पर और (यानी, सभी ब्राउजर यातायात, या सभी टेलनेट या एफटीपी यातायात), अनुप्रयोग से जाने और आने वाले सभी पैकेट का अवरोधन कर सकता है। वे अन्य पैकेट ब्लाक करते है (आमतौर पर उन्हें प्रेषक को रसीद के बिना छोड़ देते है)। सिद्धांत रूप में, आवेदन फायरवॉल सुरक्षित मशीन तक पहुचने वाले सभी अवांछित बाहरी यातायात को रोकता है।

अनुचित सामग्री के लिए सभी पैकेट पर निरीक्षण करके, फायरवॉल नेटवर्क कंप्यूटर कीड़ा और ट्रोजन के प्रसार को सीमित या रोकता है। अतिरिक्त निरीक्षण मानदंडों पैकेट के अपने गंतव्य तक अग्रेषण के लिए अतिरिक्त विलंबता जोड़ सकता हैं।

परदे के पीछे

प्रॉक्सी डिवाइस (सामान्य प्रयोजन–मशीन पर समर्पित हार्डवेयर या सॉफ्टवेयर के रूप में काम करता है) एक फायरवॉल के रूप में आवेदन के तरीके से इनपुट पैकेट (उदाहरण के लिए कनेक्शन अनुरोधों) को जवाब देता है और दूसरे पैकेट को अवरुद्ध करता है।

प्रॉक्सी बाहरी नेटवर्क से आंतरिक व्यवस्था की छेड़छाड़ को मुश्किल बनती है और एक आंतरिक व्यवस्था का दुरुपयोग से सुरक्षा नियमो को बिगाड़ती नहीं है (जब तक आवेदन प्रॉक्सी बरकरार है और ठीक से विन्यस्त है)। इसके विपरीत, घुसपैठियों एक सार्वजनिक–लग प्रणाली का अपहरण करके उसे स्वयं के प्रयोजनों के लिए एक प्रॉक्सी का प्रयोग करते है और प्रोक्सी फिर उस सिस्टम के वेश में अन्य आंतरिक मशीनों को दिखती है, जबकि आंतरिक पता रिक्त स्थान का प्रयोग सुरक्षा को बढ़ाता है, क्रैकर्स अभी भी ऐसे आईपी स्पूफिंग तरीके के रूप में काम कर सकते हैं और पैकेट को लक्ष्य नेटवर्क तक पहुँचाने का प्रयास करते है।

नेटवर्क पता अनुवाद

फायरवॉल में अक्सर नेटवर्क पता अनुवाद (NAT) की कार्यक्षमता है और मेजबान जो फायरवॉल के पीछे सुरक्षित है उनके पास सामान्यतः निजी पता रेंज होता है जो 1918 RFC में परिभाषित किया गया है। फायरवॉल के पास अक्सर संरक्षित सेनाओं के सच का पता छिपाने की कार्यशीलता होती है। मूलतः, NAT समारोह सीमित संख्या के IPv4 रौतेबल पते जो कंपनियों, व्यक्तियों उपयोग कर सकती है।

13.8.1 स्टेटलेस और स्टेटफुल पैकेट फिल्टरिंग फायरवॉलः

इस प्रकार के फायरवॉल परिनियोजन में, आंतरिक नेटवर्क राउटर फायरवॉल के माध्यम से बाहरी नेटवर्क/इंटरनेट से जुड़ा होता है। फायरवॉल डेटा पैकेट–दर–पैकेट का निरीक्षण और फिल्टर करता है। पैकेट–फिल्टरिंग फायरवॉल पैकेट्स को ज्यादातर स्रोत और/या गंतव्य IP पते, प्रोटोकॉल, स्रोत और/या गंतव्य पोर्ट संख्या और IP हेडर के भीतर विभिन्न अन्य मापदंडों जैसे मानदंडों के आधार पर अनुमति देते हैं या ब्लॉक करते हैं। निर्णय IP हेडर फील्ड जैसे ICMP संदेश प्रकार, TCP SYN और ACK बिट्स, आदि के अलावा अन्य कारकों पर आधारित हो सकता है।

पैकेट फिल्टर नियम के दो भाग हैंः

चयन मानदंडः यह निर्णय लेने के लिए एक शर्त और पैटर्न मिलान के रूप में उपयोग किया जाता है।

एक्शन फील्डः यह भाग कार्रवाई को निर्दिष्ट करता है अगर एक IP पैकेट चयन मानदंडों को पूरा करता है। कार्रवाई फायरवॉल के पार पैकेट (इंकार) या परमिट (अनुमति) हो सकती है।

पैकेट फिल्टरिंग आमतौर पर राउटर या स्विच पर एक्सेस कंट्रोल लिस्ट (ACL) को कॉन्फिगर करके पूरा किया जाता है। ACL पैकेट फिल्टर नियमों की एक तालिका है।

जैसे ही ट्रैफिक किसी इंटरफेस में प्रवेश करता है या बाहर निकलता है, फायरवॉल ACL को ऊपर से नीचे तक प्रत्येक आने वाले पैकेट पर लागू करता है, मिलान मापदंड को खोजता है और या तो व्यक्तिगत पैकेट को अनुमति या इनकार करता है।

स्टेटलेस फायरवॉल एक कठोर उपकरण का एक प्रकार है। यह पैकेट को देखता है और इसे अनुमति देता है यदि इसके मापदंड को पूरा करता है, भले ही यह किसी भी स्थापित चल रहे संचार का हिस्सा न हो।

इसलिए, इस तरह के फायरवॉल आधुनिक नेटवर्क में स्टेटफुल फायरवॉल द्वारा प्रतिस्थापित किए जाते हैं। इस प्रकार के फायरवॉल केवल ACL आधारित पैकेट निरीक्षण विधियों में से एक अधिक गहन निरीक्षण विधि प्रदान करते हैं।

स्टेटफुल फायरवॉल TCP/IP स्तर पर कनेक्शन का परीक्षण करने के लिए कनेक्शन सेटअप और टियरडाउन प्रक्रिया की निगरानी करता है। यह उन्हें कनेक्शन स्थिति का ट्रैक रखने और यह निर्धारित करने की अनुमति देता है कि कौन से मेजबान समय में किसी भी बिंदु पर खुले, अधिकृत कनेक्शन हैं।

वे नियम आधार का संदर्भ केवल तब लेते हैं जब एक नया कनेक्शन का अनुरोध किया जाता है। मौजूदा कनेक्शन से संबंधित पैकेट की तुलना ओपन कनेक्शन की फायरवॉल की अवस्था तालिका से की जाती है, और अनुमति देने या ब्लॉक करने का निर्णय लिया जाता है। यह प्रक्रिया समय की बचत करती है और अतिरिक्त सुरक्षा भी प्रदान करती है। जब तक यह पहले से ही स्थापित कनेक्शन से संबंधित नहीं है, तब तक किसी भी पैकेट को फायरवॉल को अतिक्रमण करने की अनुमति नहीं है। यह फायरवॉल पर निष्क्रिय कनेक्शन टाइमआउट कर सकता है जिसके बाद यह उस कनेक्शन के लिए पैकेट स्वीकार नहीं करता है।

13.8.2 अनुप्रयोग गेटवेः

अनुप्रयोग–स्तरीय गेटवे अनुप्रयोग–स्तरीय ट्रैफिक के लिए रिले नोड के रूप में कार्य करता है। वे इनकमिंग और आउटगोइंग पैकेट्स को इंटरसेप्ट करते हैं, प्रॉक्सी को कॉपी करते हैं और गेटवे के पार और फॉरवर्ड की गई जानकारी को चलाते हैं, और एक प्रॉक्सी सर्वर के रूप में कार्य करते हैं, किसी विश्वसनीय सर्वर या क्लाइंट और एक अविश्वासी होस्ट के मध्य किसी भी सीधे कनेक्शन को रोकते हैं। परदे के पीछे एप्लीकेशन विशिष्ट हैं। वे OSI मॉडल के एप्लिकेशन परत पर पैकेट फिल्टर कर सकते हैं।

अनुप्रयोग–विशिष्ट प्रॉक्सीः

एक अनुप्रयोग–विशिष्ट प्रॉक्सी केवल निर्दिष्ट एप्लिकेशन द्वारा उत्पन्न पैकेट को स्वीकार करता है जिसके लिए उन्हें कॉपी, फॉरवर्ड और फिल्टर करने के लिए डिजाइन किया गया है। उदाहरण के लिए, केवल एक टेलनेट प्रॉक्सी ही टेलनेट ट्रैफिक को कॉपी, फॉरवर्ड और फिल्टर कर सकता है।

यदि कोई नेटवर्क केवल एक एप्लिकेशन–स्तर गेटवे पर निर्भर करता है, तो आने वाले और बाहर जाने वाले पैकेट उन सेवाओं तक नहीं पहुँच सकते हैं, जिनमें कोई प्रॉक्सी कॉन्फिगर नहीं है। उदाहरण के लिए, यदि कोई गेटवे FTP और टेलनेट प्रॉक्सी चलाता है, तो इन सेवाओं द्वारा उत्पन्न केवल पैकेट फायरवॉल से गुजर सकते हैं। अन्य सभी सेवाएं अवरुद्ध हैं।

अनुप्रयोग–स्तर फिल्टरिंग:

एक अनुप्रयोग–स्तर प्रॉक्सी गेटवे, व्यक्तिगत पैकेट्स का परीक्षण और फिल्टर करता है, बजाय केवल उन्हें कॉपी करने और गेटवे के पार नेत्रहीन रूप से अग्रेषित करने के लिए। अनुप्रयोग–विशिष्ट प्रॉक्सिज प्रत्येक पैकेट का परीक्षण करते हैं जो गेटवे के माध्यम से गुजरता है, पैकेट की सामग्री को एप्लीकेशन परत के माध्यम से सत्यापित करता है। ये प्रॉक्सी एप्लिकेशन प्रोटोकॉल में विशेष प्रकार के कमांड्स या सूचनाओं को फिल्टर कर सकते हैं।

एप्लीकेशन गेटवे प्रदर्शन किए जाने से विशिष्ट कार्यों को प्रतिबंधित कर सकते हैं। उदाहरण के लिए, उपयोगकर्ताओं को FTP put कमांड करने से रोकने के लिए गेटवे को कॉन्फिगर किया जा सकता है। यह एक हमलावर द्वारा सर्वर पर संग्रहीत जानकारी के संशोधन को रोक सकता है।

पारदर्शक:

यद्यपि अनुप्रयोग–स्तरीय गेटवे पारदर्शी हो सकते हैं, कई कार्यान्वयनों को उपयोगकर्ता प्रमाणीकरण की आवश्यकता होती है, इससे पहले कि उपयोगकर्ता किसी अविश्वसनीय नेटवर्क तक पहुँच सकें, एक ऐसी प्रक्रिया जो पूरी पारदर्शिता को कम करती है। यदि उपयोगकर्ता आंतरिक नेटवर्क या इंटरनेट से है तो प्रमाणीकरण अलग हो सकता है। आंतरिक नेटवर्क के लिए, बाहरी अनुप्रयोगों से कनेक्ट करने के लिए IP पते की एक सरल सूची की अनुमति दी जा सकती है। लेकिन इंटरनेट की तरफ से एक मजबूत प्रमाणीकरण लागू किया जाना चाहिए।

एक एप्लिकेशन गेटवे वास्तव में दो दिशाओं (Client ↔ Proxy ↔ Server) में दो TCP कनेक्शन के मध्य TCP सेगमेंट से संबंधित है।

आउटबाउंड पैकेट के लिए, गेटवे अपने IP पते से स्रोत IP पते को बदल सकता है। इस प्रक्रिया को नेटवर्क एड्रेस ट्रांसलेशन (NAT) के रूप में जाना जाता है। यह सुनिश्चित करता है कि आंतरिक IP पते इंटरनेट के संपर्क में नहीं हैं।

13.8.3 सर्किट लेवल गेटवे:

सर्किट–स्तरीय गेटवे पैकेट फिल्टर और एप्लिकेशन गेटवे के मध्य का एक मध्यवर्ती समाधान है। यह परिवहन परत पर चलता है और इसलिए किसी भी अनुप्रयोग के लिए प्रॉक्सी के रूप में कार्य कर सकता है।

एप्लिकेशन गेटवे के समान, सर्किट–स्तरीय गेटवे भी गेटवे के पार अंत–से–अंत TCP कनेक्शन की अनुमति नहीं देता है। यह दो TCP कनेक्शन स्थापित करता है और एक नेटवर्क से दूसरे में TCP सेगमेंट को रिले करता है। लेकिन, यह एप्लिकेशन गेटवे जैसे एप्लिकेशन डेटा का परीक्षण नहीं करता है। इसलिए, कुछ समय में इसे पाइप प्रॉक्सी कहा जाता है।

SOCKS:

SOCKS (RFC 1928) सर्किट स्तर के प्रवेश द्वार को संदर्भित करता है। यह एक नेटवर्किंग प्रॉक्सी तंत्र है जो SOCKS सर्वर के एक तरफ होस्ट को सीधा IP पहुँच की आवश्यकता के बिना दूसरी तरफ होस्ट तक पूर्ण पहुँच प्राप्त करने में सक्षम बनाता है। क्लाइंट फायरवॉल पर SOCKS सर्वर से कनेक्ट होता है। तब क्लाइंट प्रमाणीकरण विधि के लिए एक बातचीत में प्रवेश करता है, और चुने हुए विधि के साथ प्रमाणीकरण करता है।

ग्राहक SOCKS सर्वर से एक कनेक्शन रिले अनुरोध भेजता है, जिसमें वांछित गंतव्य IP पता और परिवहन पोर्ट होता है। सर्वर क्लाइंट को बुनियादी फिल्टरिंग मानदंडों को पूरा करने का परीक्षण करने के बाद अनुरोध स्वीकार करता है। फिर, क्लाइंट की ओर से, गेटवे अनुरोधित अप्रकाशित होस्ट के लिए एक कनेक्शन खोलता है और फिर TCP हैंडशेकिंग की निगरानी करता है जो इस प्रकार है।

SOCKS सर्वर क्लाइंट को सूचित करता है, और सफलता के मामले में, दो कनेक्शन के मध्य डेटा को रिले करना आरंभ कर देता है। सर्किट स्तर गेटवे का उपयोग तब किया जाता है जब संगठन आंतरिक उपयोगकर्ताओं पर भरोसा करता है, और इंटरनेट पर भेजे गए सामग्री या एप्लिकेशन डेटा का निरीक्षण नहीं करना चाहता है।

13.9 DMZ के साथ फायरवॉल परिनियोजन:

फायरवॉल एक ऐसा तंत्र है जिसका उपयोग संगठनात्मक आंतरिक नेटवर्क के नेटवर्क ट्रैफिक को into और out को नियंत्रित करने के लिए किया जाता है। अधिकांश दशाओं में इन प्रणालियों में दो नेटवर्क इंटरफेस होते हैं, एक बाहरी नेटवर्क जैसे इंटरनेट और दूसरा आंतरिक पक्ष के लिए।

फायरवॉल प्रक्रिया कसकर नियंत्रित कर सकती है कि एक तरफ से दूसरी तरफ जाने की अनुमति क्या है। एक संगठन जो अपने वेब सर्वर को बाहरी पहुँच प्रदान करना चाहता है, वह पोर्ट 80 (मानक http पोर्ट) के लिए फायरवॉल की अपेक्षा आने वाले सभी ट्रैफिक को प्रतिबंधित कर सकता है। अन्य सभी ट्रैफिक जैसे मेल ट्रैफिक, FTP, SNMP, आदि को फायरवॉल में आंतरिक नेटवर्क में अनुमति नहीं है।

उपरोक्त सरल परिनियोजन में, हालांकि बाहर से अन्य सभी पहुँच अवरुद्ध हैं, एक हमलावर के लिए न केवल एक वेब सर्वर से संपर्क करना संभव है, बल्कि आंतरिक नेटवर्क पर किसी भी अन्य होस्ट ने पोर्ट 80 को दुर्घटना या अन्यथा खुला छोड़ दिया है। इसलिए, समस्या का सामना ज्यादातर संगठनों को करना है कि आंतरिक नेटवर्क की कड़ी सुरक्षा बनाए रखते हुए सार्वजनिक सेवाओं जैसे वेब, FTP और ई–मेल तक वैध पहुँच कैसे सक्षम करें। नेटवर्क में एक असैनिकीकरण क्षेत्र (DMZ) प्रदान करने के लिए विशिष्ट दृष्टिकोण फायरवॉल को तैनात कर रहा है।

इस सेटअप में, दो फायरवॉल तैनात हैं, बाहरी नेटवर्क और DMZ के मध्य एक, तथा DMZ और आंतरिक नेटवर्क के मध्य एक और। सभी सार्वजनिक सर्वर्स को DMZ में रखा गया है। इस सेटअप के साथ, फायरवॉल नियम होना संभव है जो सार्वजनिक सर्वर तक सार्वजनिक पहुँच की अनुमति देता है लेकिन आंतरिक फायरवॉल आने वाले सभी कनेक्शन को प्रतिबंधित कर सकता है। DMZ होने से, सार्वजनिक सर्वर्स को बाहरी नेटवर्क पर सीधे रखने के स्थान पर पर्याप्त सुरक्षा प्रदान की जाती है।

13.10 रोकथाम प्रणाली:

पैकेट फिल्टरिंग फायरवॉल केवल TCP/UDP/IP हेडर से जुड़े नियमों के आधार पर काम करते हैं। वे विभिन्न सत्रों के बीच सहसंबंध परीक्षण स्थापित करने का प्रयास नहीं करते हैं।

घुसपैठ का पता लगाने/रोकथाम प्रणाली (IDS/IPS) पैकेट सामग्री को देखकर डीप पैकेट निरीक्षण (DPI) करता है। उदाहरण के लिए, ज्ञात वायरस के डेटाबेस के विरूद्व पैकेट में कैरेक्टर स्ट्रिंग का परीक्षण करना, स्ट्रिंग पर हमला करना।

अनुप्रयोग गेटवे पैकेट सामग्री को देखते हैं लेकिन केवल विशिष्ट अनुप्रयोगों के लिए। वे पैकेट में संदिग्ध डेटा की तलाश नहीं करते हैं। IDS/IPS पैकेट में निहित संदिग्ध डेटा की तलाश करता है और किसी भी हमले जैसे पोर्ट स्कैनिंग, नेटवर्क मैपिंग और सेवा से वंचित करने के लिए कई पैकेट्स के मध्य सहसंबंध का परीक्षण करने की कोशिश करता है।

IDS और IPS के मध्य अंतर:

IDS और IPS नेटवर्क में विसंगतियों का पता लगाने में समान हैं। IDS एक दृश्यता उपकरण है जबकि IPS को नियंत्रण उपकरण माना जाता है। घुसपैठ का पता लगाने वाले सिस्टम नेटवर्क के किनारे बैठते हैं, कई अलग–अलग बिंदुओं पर यातायात की निगरानी करते हैं, और नेटवर्क की सुरक्षा स्थिति में दृश्यता प्रदान करते हैं। IDS द्वारा विसंगति की रिपोर्टिंग की दशा में, नेटवर्क पर नेटवर्क व्यवस्थापक या अन्य डिवाइस द्वारा सुधारात्मक कार्रवाई आरंभ की जाती है।

घुसपैठ निवारण प्रणाली फायरवॉल की तरह है और वे दो नेटवर्क के मध्य में बैठते हैं और उनके माध्यम से जाने वाले यातायात को नियंत्रित करते हैं। यह नेटवर्क ट्रैफिक में विसंगति का पता लगाने पर एक निर्दिष्ट नीति लागू करता है।

आम तौर पर, यह सभी पैकेट्स को गिरा देता है और पूरे नेटवर्क ट्रैफिक को एक विसंगति पर सूचित करता है जब तक कि व्यवस्थापक द्वारा इस तरह के विसंगति को संबोधित नहीं किया जाता है।

13.11 IDS के प्रकार:

IDS के दो बुनियादी प्रकार हैं:

1. हस्ताक्षर–आधारित IDS:

- इसे अपने हस्ताक्षर के साथ ज्ञात हमलों के डेटाबेस की आवश्यकता है।
- हस्ताक्षर एक विशेष हमले को चिह्नित करने वाले पैकेट्स के प्रकार और क्रम द्वारा परिभाषित किया गया है।
- इस प्रकार की IDS की सीमा केवल यह है कि ज्ञात हमलों का पता लगाया जा सकता है। यह IDS एक गलत अलार्म को भी फेंक सकता है। जब एक सामान्य पैकेट स्ट्रीम किसी हमले के हस्ताक्षर से मेल खाता है तो गलत अलार्म हो सकता है।
- ज्ञात सार्वजनिक ओपन–सोर्स IDS, उदाहरण Snort IDS है।

2. विसंगति आधारित IDS:

- इस प्रकार की IDS सामान्य नेटवर्क ऑपरेशन का ट्रैफिक पैटर्न बनाती है।
- IDS मोड के दौरान, यह ट्रैफिक पैटर्न को देखता है जो सांख्यिकीय रूप से असामान्य हैं। उदाहरण के लिए, ICMP असामान्य भार, पोर्ट स्कैन में घातीय वृद्धि आदि।
- किसी भी असामान्य ट्रैफिक पैटर्न का पता लगाना अलार्म उत्पन्न करता है।
- इस प्रकार की IDS तैनाती में प्रमुख चुनौती सामान्य यातायात और असामान्य यातायात के मध्य अंतर करने में कठिनाई है।

सार–संक्षेप:

नेटवर्क अभिगम नियंत्रण में दो मुख्य घटक शामिल हैं: उपयोगकर्ता प्रमाणीकरण और नेटवर्क सीमा सुरक्षा। नेटवर्क में केंद्रीय प्रमाणीकरण प्रदान करने के लिए RADIUS एक लोकप्रिय तंत्र है। फायरवॉल सार्वजनिक इंटरनेट से एक आंतरिक नेटवर्क को अलग करके नेटवर्क सीमा सुरक्षा प्रदान करता है। फायरवॉल नेटवर्क प्रोटोकॉल की विभिन्न परतों पर कार्य कर सकता है। IDS/IPS हमले का पता लगाने और उसी के विरूद्व प्रतिबंधात्मक कार्रवाई करने के लिए नेटवर्क ट्रैफिक में विसंगतियों पर नजर रखने की अनुमति देता है।

अभ्यास

1. नेटवर्क उपकरणों तक पहुँच कैसे सुरक्षित की जा सकती है?
2. उपयोगकर्ता प्रमाणीकरण और प्रमाणन क्या हैं?
3. पासवर्ड (पारण शब्द) आधारित प्रमाणीकरण क्या होता है?
4. केन्द्रीकृत प्रमाणीकरण विधि को लिखिए।
5. एक्सेस (अभिगम) नियंत्रण सूची क्या है?
6. निम्न पर टिप्पणी लिखिए:
   कम्प्यूटर वायरस, एण्टी वायरस, फायरवॉल
7. स्टेटलेस और स्टेटफुल पैकेट फिल्टरिंग फायरवॉल से क्या समझते हैं?
8. निम्न पर टिप्पणी लिखिए:
   अनुप्रयोग गेटवे (द्वार), सर्किट लेवल गेटवे (परिपथ स्तरीय द्वार)
9. DMZ के साथ फायरवॉल परिनियोजन कैसे किया जाता है?
10. IDS के प्रकार बताइए।

परिशिष्ट

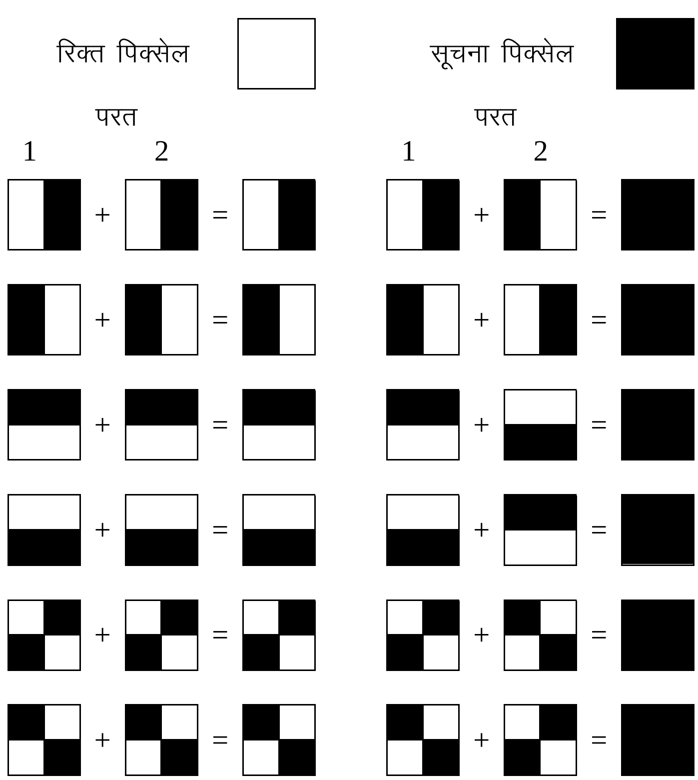
1. विजुअल क्रिप्टोग्राफीः

विजुअल क्रिप्टोग्राफी एक विशेष एन्क्रिप्शन तकनीक है जो छवियों को इस तरह से छिपाने के लिए है कि अगर सही कुंजी छवि का उपयोग किया जाता है तो इसे मानवीय दृष्टि से डिक्रिप्ट किया जा सकता है। यह तकनीक 1994 में नोर और शमीर द्वारा प्रस्तावित की गई थी। विजुअल क्रिप्टोग्राफी दो पारदर्शी छवियों का उपयोग करती है। एक छवि में यादृच्छिक पिक्सेल होते हैं और दूसरी छवि में गुप्त जानकारी होती है। छवियों में से किसी एक से गुप्त जानकारी प्राप्त करना असंभव है। जानकारी को प्रकट करने के लिए पारदर्शी छवियों या परतों दोनों की आवश्यकता होती है। विजुअल क्रिप्टोग्राफी को लागू करने का सबसे आसान तरीका दो परतों को एक पारदर्शी शीट पर प्रिंट करना है।

जब रैंडम इमेज में ट्रिमली रैंडम पिक्सल होते हैं, तो इसे वन–टाइम पैड सिस्टम के रूप में देखा जा सकता है और यह अनब्रेकेबल एनक्रिप्शन पेश करेगा। ओवरले एनीमेशन में हम दो परतों को एक–दूसरे पर फिसलते हुए देख सकते हैं जब तक कि वे सही ढंग से संरेखित न हों और छिपी हुई जानकारी दिखाई दे। इसे स्वयं आजमाने के लिए, आप उदाहरण परतों 1 और 2 को कॉपी कर सकते हैं, और उन्हें एक पारदर्शी शीट या पतले कागज पर प्रिंट कर सकते हैं। हमेशा एक प्रोग्राम का उपयोग करें जो काले और सफेद पिक्सेल को सही ढंग से प्रदर्शित करता है और प्रिंटर सेट करता है ताकि सभी पिक्सेल सटीक रूप से मुद्रित हों (कोई प्रसार या फोटो वृद्धि आदि)। हम पेंट जैसे ड्राइंग प्रोग्राम में उन्हें एक दूसरे पर कॉपी और पेस्ट भी कर सकते हैं और तुरंत परिणाम देख सकते हैं, लेकिन पारदर्शी ड्राइंग का चयन करना और दोनों परतों को एक–दूसरे के ऊपर बिल्कुल संरेखित करना सुनिश्चित करें।

विजुअल क्रिप्टोग्राफी कैसे काम करता है?

छवियों के प्रत्येक पिक्सेल को छोटे ब्लॉकों में विभाजित किया गया है। हमेशा समान संख्या में सफेद (पारदर्शी) और काले ब्लॉक होते हैं। यदि पिक्सेल को दो भागों में विभाजित किया जाता है, तो एक सफेद और एक काला ब्लॉक होता है। यदि पिक्सेल को चार समान भागों में विभाजित किया जाता है, तो दो सफेद और दो काले ब्लॉक होते हैं। ऊपर से उदाहरण की छवियां पिक्सेल का उपयोग करती हैं जिन्हें चार भागों में विभाजित किया गया है।



उपरोक्त चित्र में हम देख सकते हैं कि चार भागों में विभाजित एक पिक्सेल में छह अलग–अलग अवस्थाएँ हो सकती हैं। यदि परत 1 पर एक पिक्सेल में एक दी गई अवस्था है, तो परत 2 पर पिक्सेल में दो में से एक अवस्था हो सकती है समान या परत 1 के पिक्सेल का उल्टा। यदि परत 2 का पिक्सेल परत 1 के समान है, तो ओवरलेड पिक्सेल आधा काला और आधा सफेद होगा। ऐसे ओवरले पिक्सेल को ग्रे या खाली कहा जाता है। यदि लेयर 1 और 2 के पिक्सल उलटे या विपरीत हैं, तो ओवरले संस्करण पूरी तरह से काला हो जाएगा। यह एक सूचना पिक्सेल है।

अब हम दो लेयर्स बना सकते हैं। एक पारदर्शी छवि, परत 1, में पिक्सेल होते हैं, जिनमें सभी एक यादृच्छिक अवस्था होते हैं, छह संभावित स्थितियों में से एक। परत 2 परत 1 के समान है, ओवरले होने पर उन पिक्सेल को छोड़कर, जो काले होने चाहिए (जानकारी होनी चाहिए)। इन पिक्सेल में एक स्थिति होती है जो परत 1 में समान पिक्सेल के विपरीत होता है। यदि दोनों छवियों को ओवरले किया गया है, तो समान अवस्था वाले क्षेत्र ग्रे दिखाई देंगे, और विपरीत अवस्थाओं वाले क्षेत्र काले होंगे।

पिक्सेल की प्रणाली को विभिन्न तरीकों से लागू किया जा सकता है। हमारे उदाहरण में, प्रत्येक पिक्सेल को चार ब्लॉकों में विभाजित किया गया है। हालाँकि, हम पिक्सेल का उपयोग भी कर सकते हैं, जिसे दो आयत खंडों में विभाजित किया गया है, या यहाँ तक कि विभाजित वृत्त भी। इसके अलावा, इससे कोई फर्क नहीं पड़ता कि पिक्सेल क्षैतिज या लंबवत रूप से विभाजित है। कई अलग–अलग पिक्सेल सिस्टम हैं, कुछ बेहतर कंट्रास्ट, उच्च रिजॉल्यूशन या यहां तक कि रंग पिक्सेल के साथ भी।

यदि लेयर 1 के पिक्सेल अवस्था सही मायने में (क्रिप्टो सिक्योर) यादृच्छिक हैं, तो लेयर 2 के खाली और सूचना पिक्सल दोनों में भी पूरी तरह से यादृच्छिक अवस्था होंगे। कोई यह नहीं जान सकता है कि परत 2 में एक पिक्सेल का उपयोग एक ग्रे या ब्लैक पिक्सेल बनाने के लिए किया जाता है, क्योंकि हमें ओवरले परिणाम जानने के लिए परत 1 में उस पिक्सेल की स्थिति की आवश्यकता होती है (जो यादृच्छिक है)। यदि सत्य यादृच्छिकता के लिए सभी आवश्यकताओं को पूरा किया जाता है, तो विजुअल क्रिप्टोग्राफी सूचना सिद्धांत के अनुसार पूर्ण गोपनीयता प्रदान करता है।

यदि विजुअल क्रिप्टोग्राफी का उपयोग सुरक्षित संचार के लिए किया जाता है, तो प्रेषक रिसीवर को अग्रिम में एक या एक से अधिक यादृच्छिक परतें वितरित करेगा। यदि प्रेषक के पास एक संदेश है, तो वह एक विशेष वितरित परत 1 के लिए एक परत 2 बनाता है और इसे प्राप्तकर्ता को भेजता है। प्राप्तकर्ता दो परतों को संरेखित करता है और गुप्त जानकारी का पता चलता है, यह एन्क्रिप्शन डिवाइस, कंप्यूटर या हाथ से गणना करने की आवश्यकता के बिना होता है। यह प्रणाली अटूट है, जब तक कि दोनों परतें गलत हाथों में न पड़ें। जब दोनों परतों में से एक को प्रतिच्छेदित किया जाता है तो एन्क्रिप्टेड जानकारी को पुनः प्राप्त करना असंभव है। विजुअल क्रिप्टोग्राफी इसलिए भी सुरक्षित गुप्त विभाजन का एक रूप है जहां मूल जानकारी को पुनः प्राप्त करने के लिए दो गुप्त साझेदारों की आवश्यकता होती है।

सूचना छिपाने के स्पष्ट अनुप्रयोग के अलावा, विजुअल क्रिप्टोग्राफी को कई डोमेन जैसे कि एक्सेस कंट्रोल (बैंक वॉल्ट खोलना), दहलीज पर हस्ताक्षर (कई उपकरणों जैसे बिटकॉइन के माध्यम से वॉलेट सुरक्षा), कॉपीराइट सुरक्षा, वॉटरमार्किंग, विजुअल ऑथेंटिकेशन पर लागू किया जा सकता है। टिकट सत्यापन, और मानव पहचान, आदि विजुअल क्रिप्टोग्राफी अनुप्रयोगों बैंकिंग उद्योग से उपग्रह इमेजिंग, एकत्र बॉयोमीट्रिक डेटा के संरक्षण के लिए वाणिज्यिक अनुप्रयोग के लिए सीमा होती है। विजुअल क्रिप्टोग्राफी तकनीक उपयोगकर्ता के लिए बहुत सहज है।

ऑनलाइन मनी ट्रांसफर को सुरक्षित करने के लिए, उपयोगकर्ता को ट्रांजेक्शन सर्वर से कई पारदर्शिता प्राप्त होती है। सर्वर उपयोगकर्ता के स्क्रीन पर लेनदेन डेटा युक्त एक विजुअल संदेश भेजता है, और यह विजुअल क्रिप्टोग्राफी के माध्यम से एन्कोडेड है। यदि उपयोगकर्ता एन्कोडेड छवि के शीर्ष पर एक निश्चित संख्या के साथ पारदर्शिता रखता है, तो स्क्रीनिंग व्यक्ति छवि के भीतर निहित संदेश देख सकता है। जब सर्वर को सही TAN प्राप्त होता है तो वह लेन–देन निष्पादित करता है, अन्यथा नहीं। इस तरह, कोई भी प्रकृति में बैंकिंग लेनदेन को अधिक सुरक्षित बना सकता है। विशेष रूप से, विजुअल क्रिप्टोग्राफी Moiré पैटर्न और वॉटरमार्किंग के उपयोग में लोकप्रिय है। Moirés पैटर्न उत्पन्न होते हैं जब एक खुलासा परत एक छवि के शीर्ष पर समय–समय पर दोहराया आकृतियों के साथ उपलब्ध होती है।

शेयरों को अलग करने पर शेयरों को सुपरइम्पोज करके मूल रहस्य का खुलासा किया जा सकता है, एम्बेडेड छवि देखी जा सकती है। विजुअल क्रिप्टोग्राफी के लिए एक और अक्सर उपयोग किया जाने वाला अनुप्रयोग वॉटरमार्किंग है। वॉटरमार्किंग सूचना छुपाने और एम्बेड करने में एक महत्वपूर्ण भूमिका निभाता है। पारंपरिक विजुअल क्रिप्टोग्राफी के समान, वॉटरमार्किंग में विजुअल क्रिप्टोग्राफी का कार्यान्वयन आधार मैट्रिक्स पर आधारित है और अंतिम बरामद रहस्य को सफेद और काले रंगों के बीच विपरीत का उपयोग करके माना जाता है। इसी तरह, विजुअल क्रिप्टोग्राफी के भीतर वॉटरमार्क के उपयोग का भी पता लगाएं। उत्पादों में विजुअल क्रिप्टोग्राफी आधारित वॉटरमार्किंग को एम्बेड करना, धोखाधड़ी को रोकने का एक प्रभावी तरीका है, खासकर उन डोमेन में जहां वॉटरमार्किंग के उपयोग से पहले से ही लाभ मिलता है। समायोजन, आकार और विशेष उपकरणों की लागत जैसी कठिनाइयों के कारण, इन सुझावों से उन अनुप्रयोगों का नेतृत्व नहीं हुआ जो गंभीर उद्देश्यों के लिए उपयोग किए जाते हैं। लेकिन भविष्य में, विभिन्न दृष्टिकोणों और साथ ही नए विचारों में प्रस्तुत विचारों के आगे के विकास, विजुअल क्रिप्टोग्राफी के व्यावहारिक अनुप्रयोगों को फैला सकते हैं। वर्तमान समय इमेज हैचिंग तकनीक के साथ विजुअल क्रिप्टोग्राफी मुद्रा उद्योग में विजुअल क्रिप्टोग्राफी के विस्तार की अनुमति देगा, जैसे कि बैंकिंग उद्योग के भीतर। सुरक्षित मुद्रण उद्योग के भीतर शेयरों के उपयोग पर भी विचार किया जाना चाहिए। एक कंप्यूटर सिस्टम में एक शेयर को स्कैन करना और फिर इसके संबंधित हिस्से को डिजिटल रूप से सुपरइम्पोज करना भी माना जा सकता है।

2. क्वांटम क्रिप्टोग्राफी:

क्वांटम क्रिप्टोग्राफी, क्रिप्टोग्राफिक कार्यों को करने के लिए क्वांटम यांत्रिक गुणों का दोहन करने का विज्ञान है। क्वांटम क्रिप्टोग्राफी का सबसे अच्छा उदाहरण क्वांटम कुंजी वितरण है जो प्रमुख एक्सचेंज समस्या के लिए एक सूचना–सैद्धांतिक रूप से सुरक्षित समाधान प्रदान करता है। क्वांटम क्रिप्टोग्राफी का लाभ इस तथ्य में निहित है कि यह विभिन्न क्रिप्टोग्राफिक कार्यों को पूरा करने की अनुमति देता है जो केवल शास्त्रीय (यानी गैर–क्वांटम) संचार का उपयोग करके असंभव साबित या अनुमानित हैं। उदाहरण के लिए, एक क्वांटम स्थिति में एन्कोड किए गए डेटा की प्रतिलिपि बनाना असंभव है। यदि कोई एन्कोडेड डेटा को पढ़ने का प्रयास करता है, तो क्वांटम स्थिति को बदल दिया जाएगा (नो–क्लोनिंग प्रमेय)। इसका उपयोग क्वांटम कुंजी वितरण में ईव्सड्रॉपिंग का पता लगाने के लिए किया जा सकता है।
क्वांटम क्रिप्टोग्राफी पारंपरिक क्रिप्टोग्राफिक प्रणालियों से अलग है जिसमें यह गणित पर निर्भर करता है, बल्कि गणित पर निर्भर करता है, अपने सुरक्षा मॉडल के प्रमुख पहलू के रूप में।

क्वांटम क्रिप्टोग्राफी प्रकाश के अलग–अलग कणों/तरंगों (फोटॉन) और उनके आंतरिक क्वांटम गुणों के उपयोग पर आधारित है ताकि एक अटूट क्रिप्टोसिस्टम विकसित किया जा सके – अनिवार्य रूप से क्योंकि उस सिस्टम को परेशान किए बिना किसी भी सिस्टम की क्वांटम स्थिति को मापना असंभव है। यह सैद्धांतिक रूप से संभव है कि अन्य कणों का उपयोग किया जा सकता है, लेकिन फोटॉन आवश्यक सभी आवश्यक गुणों की पेशकश करते हैं, उनका व्यवहार तुलनात्मक रूप से अच्छी तरह से समझा जाता है, और वे ऑप्टिकल फाइबर केबल्स में सूचना वाहक हैं, जो बेहद उच्च–बैंडविड्थ संचार के लिए सबसे आशाजनक माध्यम हैं।

क्वांटम क्रिप्टोग्राफी कैसे कार्य करता है?

मान लें कि दो लोग A और B सुरक्षित रूप से संदेश का आदान–प्रदान करना चाहते हैं। A, B को एक कुंजी भेजकर संदेश शुरू करता है, जो संदेश डेटा को एन्क्रिप्ट करने के लिए मोड होगा। यह बिट्स का एक यादृच्छिक क्रम है, जो एक निश्चित प्रकार की योजना का उपयोग करके भेजा जाता है, जो दो अलग–अलग प्रारंभिक मूल्यों को देख सकता है एक विशेष बाइनरी मान (0 या 1) का प्रतिनिधित्व करता है।

आइए हम मान लें कि यह कुंजी एक दिशा में घूमने वाले फोटोन की एक धारा है, इनमें से प्रत्येक फोटॉन कणों में एक बिट डेटा (या तो 0 या 1) का प्रतिनिधित्व करता है। हालांकि, उनकी रैखिक यात्रा के अलावा, ये सभी फोटॉन एक निश्चित तरीके से दोलन (कंपन) कर रहे हैं। ये दोलन किसी भी बोधगम्य धुरी के पार किसी भी 360 डिग्री रेंज में हो सकते हैं, लेकिन सादगी के उद्देश्य (कम से कम जहां तक क्वांटम क्रिप्टोग्राफी में चीजों को सरल बनाना संभव है) के लिए, आइए हम मान लें कि उनके दोलनों को 4 विशेष में वर्गीकृत किया जा सकता है।

हम इन्हें UP/DOWN, LEFT/RIGHT, UPLEFT/RIGHTDOWN और UPRIGHT/LEFTDOWN के रूप में परिभाषित करेंगे। इस कंपन के कोण को फोटॉन के ध्रुवीकरण के रूप में जाना जाता है। अब, हम समीकरण में एक ध्रुवीकरण शुरू करते हैं। एक पोलराइजर बस एक फिल्टर है जो कुछ फोटॉन को पहले के समान दोलन के माध्यम से इसके माध्यम से गुजरने की अनुमति देता है और दूसरों को दोलन की एक बदली हुई स्थिति से गुजरने देता है (यह कुछ फोटॉन को पूरी तरह से अवरुद्ध भी कर सकता है, लेकिन आइए इस अभ्यास के लिए उस गुण को अनदेखा करें)। A में एक पोलराइजर होता है जो वर्णित चार अवस्थाओं में से किसी एक में फोटॉनों को प्रसारित कर सकता है – वास्तव में, वह या तो आयताकार (UP/DOWN और LEFT/RIGHT) या विकर्ण (UPLEFT/RIGHTDOWN और UPRIGHT/LEFTDOWN) ध्रुवीकरण फिल्टर चुन सकता है।

A एक यादृच्छिक तरीके से प्रत्येक एकल फोटॉन बिट के संचरण के लिए रेक्टिलाइनर और विकर्ण फिल्टर के बीच उसकी ध्रुवीकरण योजना को स्वैप करता है। ऐसा करने में, ट्रांसमिशन में दो ध्रुवीकरणों में से एक हो सकता है, एक एकल बिट का प्रतिनिधित्व करता है, या तो 1 या 0, या तो योजना में वह उपयोग करता है।

फोटॉन कुंजी प्राप्त करते समय, B को अपने आयताकार या विकर्ण ध्रुवीय का उपयोग करके प्रत्येक फोटॉन बिट को मापने का चयन करना होगा, कभी–कभी वह सही ध्रुरुवीकरण का चयन करेगा और अन्य समय पर वह गलत का चयन करेगा। ऐलिस की तरह, वह एक यादृच्छिक तरीके से प्रत्येक ध्रुवीय का चयन करता है। तो जब गलत पोलराइजर चुना जाता है तो फोटोन के साथ क्या होता है?

हाइजेनबर्ग अनिश्चितता सिद्धांत बताता है कि हम नहीं जानते कि प्रत्येक व्यक्ति फोटॉन का क्या होगा, इसके व्यवहार को मापने के लिए, हम इसके गुणों में परिवर्तन करते हैं (इस तथ्य के अलावा कि अगर किसी प्रणाली के दो गुण हैं जो हम चाहते हैं मापने के लिए, एक मापना हमें दूसरे की मात्रा निर्धारित करने से रोकता है)। हालाँकि, हम एक अनुमान लगा सकते हैं कि एक समूह के रूप में उनके साथ क्या होता है। मान लीजिए B, UPLEFT/RIGHTDOWN और UPRIGHT/LEFTDOWN (विकर्ण) फोटॉनों को मापने के लिए एक आयताकार ध्रुरुवीकरण का उपयोग करता है। यदि वह ऐसा करता है, तो फोटॉनों को एक बदली हुई अवस्था से गुजारा जाएगा – यानी आधा UP/DOWN में और दूसरा आधा LEFT/RIGHT में बदल जाएगा। लेकिन हम यह नहीं जान सकते हैं कि कौन से व्यक्तिगत फोटोन किस राज्य में बदल जाएंगे (यह भी एक वास्तविकता है कि कुछ फोटोन को वास्तविक दुनिया के आवेदन में पूरी तरह से पास होने से रोका जा सकता है, लेकिन यह सिद्धांत के लिए प्रासंगिक नहीं है)।

बॉब कुछ फोटॉन को सही तरीके से मापता है और अन्य गलत तरीके से। इस बिंदु पर, A और B संचार का एक चैनल स्थापित करते हैं जो असुरक्षित हो सकता है – अर्थात, अन्य लोग A में सुन सकते हैं, फिर B को सलाह देने के लिए आगे बढ़ते हैं कि वह किस पोलराइजर को प्रत्येक फोटॉन बिट भेजती थी – लेकिन यह नहीं कि वह प्रत्येक को कैसे ध्रुवीकृत करती है। तो वह कह सकता है कि फोटो नंबर 8597 (सैद्धांतिक रूप से) को रेक्टिलाइनर स्कीम का उपयोग करके भेजा गया था, लेकिन वह यह नहीं कहेगी कि उसने UP/DOWN या LEFT/RIGHT भेजा है या नहीं। B ने पुष्टि की कि क्या उन्होंने प्रत्येक विशेष फोटोन को प्राप्त करने के लिए सही ध्रुवीकरण का उपयोग किया है। A और B तब सभी फोटॉन मापों को त्याग देते हैं जिन्हें उन्होंने जांचने के लिए गलत ध्रुवीकरण का उपयोग किया था। उनके पास क्या है, औसतन, 0 और 1 का एक अनुक्रम जो मूल संचरण की लंबाई की आधी है ... लेकिन यह एक बार के पैड के लिए आधार बनाएगा, एकमात्र क्रिप्टोसिस्टम है, जिसे यदि ठीक से लागू किया गया है, तो यह है पूरी तरह से यादृच्छिक और सुरक्षित साबित हुआ।

अब, मान लीजिए कि हमारे पास एक ईव्सड्रोपर, E है, जो सुनने का प्रयास करता है, वही ध्रुवीकरण करता है जो B करता है और यह भी बेतरतीब ढंग से चुनना चाहिए कि प्रत्येक फोटॉन के लिए रेक्टिलियर या विकर्ण का उपयोग करना है या नहीं। हालाँकि, वह भी उसी समस्या का सामना करती है जो B करता है, उस आधे समय में वह गलत ध्रुवीकरण का चयन करेगा। लेकिन B को A से बात करने का लाभ यह पुष्टि करने के लिए है कि प्रत्येक फोटॉन के लिए किस ध्रुवीकरण प्रकार का उपयोग किया गया था। यह E के लिए बेकार है, आधे समय के रूप में उसने गलत डिटेक्टर का इस्तेमाल किया और कुछ फोटॉनों की गलत व्याख्या करेगा जो उस अंतिम कुंजी का निर्माण करेंगे, जो इसे बेकार कर देगा।

इसके अलावा, क्वांटम क्रिप्टोग्राफी में निहित सुरक्षा का एक और स्तर है – घुसपैठ का पता लगाना। A और B को पता चल जाता कि क्या E उन पर झपट रहा था। तथ्य यह है कि E 'फोटॉन हाईवे' पर है निम्नलिखित के कारण स्पष्ट हो सकता है।

मान लें कि A फोटॉन संख्या 349 को UPRIGHT/LEFTDOWN के रूप में B तक पहुंचाता है, लेकिन उस के लिए, E रेक्टिलिनियर पोलराइजर का उपयोग करता है, जो केवल UP/DOWN या LEFT/RIGHT फोटॉनों को सही तरीके से माप सकता है। E क्या करेगा उस फोटॉन को UP/DOWN या LEFT/RIGHT में बदल देगा, क्योंकि यही एकमात्र तरीका है जिससे फोटॉन पास हो सकता है। यदि B अपने रेक्टिलिनियर पोलराइजर का उपयोग करता है, तो इससे कोई फर्क नहीं पड़ेगा कि वह क्या उपाय करता है क्योंकि पोलराइजर चेक A और B ऊपर से गुजरता है, उस फोटॉन को अंतिम कुंजी से हटा देगा। लेकिन अगर वह विकर्ण ध्रुवीकरण का उपयोग करता है, तो एक समस्या उत्पन्न होती है जब वह इसके ध्रुवीकरण को मापता है, वह इसे सही ढंग से UPRIGHT/LEFTDOWN के रूप में माप सकता है, लेकिन वह एक समान मौका है, उसे हाइजेनबर्ग अनिश्चितता सिद्धांत के अनुसार, गलत तरीके से UPLEFT/RIGHTDOWN के रूप में मापता है। E के गलत ध्रुवीकरण का उपयोग उस फोटॉन को ताना देगा और B को सही ध्रुवीकरण का उपयोग करने पर भी त्रुटियां करने का कारण होगा।

E के गलत इरादों को खोजने के लिए, उन्हें उपरोक्त प्रक्रियाओं को पूरा करना होगा, जिसके साथ वे 0s और 1s के समरूप कुंजी क्रम पर पहुंचेंगे – जब तक कि किसी को ईर्ष्या नहीं हुई है, जहां कुछ विसंगतियां होंगी। फिर उन्हें अपनी कुंजी की वैधता की जांच करने के लिए और उपाय करने होंगे।

मान लेते हैं कि अंतिम कुंजी में 4,000 बाइनरी अंक शामिल हैं। क्या करने की आवश्यकता है कि इन अंकों के एक सबसेट को A और B द्वारा यादृच्छिक रूप से चुना जाए, दोनों स्थिति (यानी, अंकों की संख्या 2, 34, 65, 911 आदि) और अंक स्थिति (0) के संदर्भ में, 200 अंक कहें या 1। A और B इनकी तुलना करते हैं – यदि वे मेल खाते हैं, तो वास्तव में कोई मौका नहीं है कि E सुन रहा था। हालांकि, अगर वह सुन रहा था, तो उसके अनदेखे होने की संभावना अनगिनत खरबों में एक है, यानी वास्तविक दुनिया में कोई मौका नहीं। A और B को पता होगा कि कोई व्यक्ति सुन रहा था और फिर कुंजी का उपयोग नहीं करेगा – उन्हें E के लिए दुर्गम एक सुरक्षित चैनल पर फिर से कुंजी विनिमय शुरू करने की आवश्यकता होगी, भले ही A और B के बीच तुलना ऊपर अभी भी की जा सकती है असुरक्षित चैनल। हालाँकि, भले ही A और B ने निष्कर्ष निकाला हो कि उनकी कुंजी सुरक्षित है, क्योंकि उन्होंने एक असुरक्षित चैनल पर 200 अंकों का संचार किया है, इन 200 अंकों को अंतिम कुंजी से त्याग दिया जाना चाहिए, इसे 4,000 से 3,800 बिट कुंजी में बदल दिया जाता है।

शब्द संग्रह

अंग्रेजी शब्द	मूल रूप	हिन्दी वर्तनी
Access Control	एक्सेस कन्ट्रोल	अभिगम नियंत्रण
Adjacent	ऐडजेकेन्ट	आसन्न
Algoritham	एल्गोरिथ्म	कलनविधि
Application Gateways	एप्लीकेशन गेटवे	अनुप्रयोग द्वार
Application Layer	एप्लीकेशन लेयर	अनुप्रयोग परत
Assignment	एसाइनमेन्ट	अभिहस्तांकन
Asymmetric Key Encryption	एसिमेट्रिक की एन्क्रिप्शन	असममित कुंजी कूट प्रक्रिया
Block Cipher	ब्लॉक सिफर	खण्ड कूटलेख
Certificate Authority	सर्टिफिकेट अथॉरिटी	प्रमाणपत्र प्राधिकारी
Certifying Authority	सर्टिफाइंग अथॉरिटी	प्रमाणन प्राधिकरण
Checksum	चेकसम	जाँच योग
Cipher	सिफर	कूटलेख
Cipher Block	सिफर ब्लॉक	कूटलेख खण्ड
Ciphertext	सिफर–टेक्स्ट	कूटलेख–पाठ
Circuit-Level Gateway	सर्किट लेवल गेटवे	परिपथ स्तरीय द्वार
Cleartext	क्लीयर–टेक्स्ट	स्पष्ट–पाठ
Coded	कोडेड	कूट
Communication	कम्यूनिकेशन	संचार
Computation	कम्प्यूटेशन	संगणन
Counter	काउन्टर	गणित्र
Cryptanalysis	क्रिप्टैनालिसिस	कूटविश्लेषण
Cryptanalytic	क्रिप्टैनालिटिक	कूटविश्लेषिक
Cryptographic	क्रिप्टोग्राफी	कूटलेखन
Cryptography	क्रिप्टोग्राफिक	कूटलेखीय
Cryptology	क्रिप्टोलॉजी	कूटलिपि
Cryptosystem	क्रिप्टोसिस्टम	कूटतंत्र, कूटप्रणाली
Data Link Layer	डेटा लिंक लेयर	आंकड़ा कड़ी परत
Decode	डीकोड	अकूट
Decryption	डिक्रिप्शन	अकूट प्रक्रिया
Deterministic cipher	डिटरमिनिस्टिक सिफर	नियतात्मक कूटलेख
Digital Certificate	डिजिटल सर्टिफिकेट	अंकीय प्रमाण पत्र
Digital Signatures	डिजिटल सिग्नेचर	अंकीय हस्ताक्षर
Elliptic Curve Cryptography	एलिप्टिक–कर्व क्रिप्टोग्राफी	अण्डाकार–वक्र कूटलेखन
Encoding	एन्कोडिंग	कूटन
Encrypt	एन्क्रिप्ट	कूटित
Encrypted Hash	एन्क्रिप्टेड हैश	कूटित द्रुतान्वेषण
Encrypting function	एन्क्रिप्टिंग फंक्शन	कूटित फलन
Encryption	एन्क्रिप्शन	कूट प्रक्रिया
Hash Function	हैश फंक्शन	द्रुतान्वेषण फलन
Input	इनपुट	निवेश
Integrity	इंटिग्रिटि	अखंडता
Interceptor	इंटरसेप्टर	अवरोधक
Key	की	कुंजी

Key-Stream	की–स्ट्रीम	कुंजी–प्रवाह
Manual System	मैनुअल सिस्टम	दस्ती प्रणाली
Matrix	मैट्रिक्स	आव्यूह
Message Digest	मैसेज डाइजेस्ट	संदेश पाचन
Network Layer	नेटवर्क लेयर	जालक्रम परत
Non-invertible	नॉन–इन्वरटिबल	अव्युत्क्रमणीय
Output	आउटपुट	निर्गत
Padding	पैडन	पैडन
Parity Bits	पैरिटि बिट्स	समता बिट्स
Physical Layer	फिजिकल लेयर	भौतिक परत
Plaintext	प्लेन–टेक्स्ट	साधारण–पाठ
Presentation Layer	प्रजेन्टेशन लेयर	प्रस्तुतिकरण परत
Private Key	प्राइवेट की	व्यक्तिगत कुंजी
Processing	प्रोसेसिंग	प्रसंस्करण
Protocol	प्रोटोकॉल	संदेशाचार
Public Key	पब्लिक की	सार्वजनिक कुंजी
Public Key Infrastructure	पब्लिक की इन्फ्रास्ट्रक्चर	सार्वजनिक कुंजी अवसंरचना
Quantum Bit	क्वांटम बिट्स	क्वांटम बिट्स
Registration Authority	रजिस्ट्रेशन अथॉरिटी	पंजीकरण प्राधिकरण
Secure Shell Protocol	सिक्योर शेल प्रोटोकॉल	सुरक्षित शेल संदेशाचार
Secure Socket Layer	सिक्योर सॉकेट लेयर	सुरक्षित सॉकेट परत
Security	सिक्योरिटी	सुरक्षा
Session Layer	सेशन लेयर	सत्र परत
Stegnography	स्टेग्नोग्राफी	गुप्त लेखन
Stream Cipher	स्ट्रीम सिफर	प्रवाह कूटलेख
Substitution	सबस्टीट्यूशन	प्रतिस्थापन
Symmetric Key Encryption	सिमेट्रिक की एन्क्रिप्शन	सममित कुंजी एन्क्रिप्शन
Synchronize	सिन्क्रोनाइज	तुल्यकालन
Transmission	ट्रांसमिशन	संचरण
Transport Layer	ट्रांसपोर्ट लेयर	परिवहन परत
Validation Authority	वेलिडेशन अथॉरिटी	सत्यापन प्राधिकरण
Wired	वायर्ड	तारयुक्त
Wireless	वायरलेस	तार रहित

संदर्भ ग्रंथ

1. William Stallings': **Cryptography and Network Security**, Pearson, 5 edition, 2010.
2. Behrouz A. Forouzan: **Cryptography & Network Security**, McGraw-Hill, 1 edition, 2007.
3. Atul Kahate, **Cryptography and Network Security**, McGraw-Hill, India, Second Edition, 2009.